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

Hybrid Attribute Based Symmetric Encryption Algorithm for Enhanced Access Polices in Medical Wireless Sensor Networks

B. Naresh Kumar[1], M. Srinivas*[2]

Submitted: 25/04/2023 **Revised**: 25/06/2023 **Accepted**: 06/07/2023

Abstract: Medical wireless sensor network (MWSN) is a vital component of the Internet of Things (IoT). It enables the transmission of health data between smart devices and sensor nodes. The integration of this technology has many advantages, but it is also important to ensure that the confidentiality of the information is maintained. The paper presents a framework that aims to establish a secure mechanism for managing the massive amount of medical data collected by sensor nodes in the MWSN. It aims to establish communication channels between patients and doctors during emergencies and in normal situations. The framework proposes a method that uses attribute-based and symmetric encryption techniques to enhance the confidentiality and integrity of the data collected by sensor nodes in the MWSN. The system's efficiency was demonstrated through simulations. The research conducted by the team provides a framework that can be used to establish a secure mechanism for managing the data collected by sensor nodes in the MWSN. This technology could help improve the quality of healthcare services.

Keywords: *MWSN, Encryption, Data Confidentiality, Integrity*

1. Introduction

The management of electronic health records with the WSN can improve the quality of care and lower costs [1]. The use of the MWSN can transform healthcare by connecting various sensors and devices to provide remote monitoring and care for patients. It can also help lower medical costs. However, the security and privacy of the data collected by the MWSN can be compromised. This is because the vast amount of data that is stored in cloud servers can be vulnerable to eavesdropping and tampering.

One of the biggest challenges that the MWSN faces is ensuring that the security of the data collected by it is not compromised. This is done with remote access control [2]-[4]. Medical data is encrypted and placed in the cloud to protect its confidentiality. Although ABE is commonly used for sensor data encryption, its complexity makes it unsuitable for the MWSN.

Due to the nature of the sensor devices, there is a need to create low-complexity and efficient mechanisms for protecting medical data. Medical data must be protected using low-complexity encryption methods [5]-[7]. The power consumption and computational capabilities of sensor devices are typically limited. Therefore, efficient and low-complex encryption methods for protecting medical data must be created [8]-[9].

The goal of this paper is to develop architecture for the management of medical data in the WSN. This will allow for secure communication between patients and doctors in both emergency and normal conditions. The paper is divided into six sections. Section 2 explores the different aspects of data management within the WSN. Section 3 explores the architecture for data encryption within the framework. Section 4 presents the security model for the MWSN, and Section 5 summarizes the findings from the simulation. Section 6 wraps up the research work.

2. Literature Survey

The rapid emergence and evolution of wireless sensor networks and the integration of the Internet of Things have greatly changed the way various industries and sectors operate [10]. For instance, the healthcare industry has started to embrace the use of IoT technology. This has led to the development of new concepts such as the Internet of Things Medical and Industrial IoT [11-13]. These innovations can help improve the efficiency and connectivity of various applications. The outbreak of COVID-19 has highlighted the importance of telemedicine in the healthcare industry [14]. Through the integration of biosensors and the Internet, real-time monitoring of health can be carried out through the use of smart devices. Patients can also benefit from the remote operation of various smart equipment, such as insulin delivery systems and pacemakers [15]. Due to the increasing number of smart devices and the complexity of their operation, there has been a rise in the number of attacks on cloud

[1]*Research scholar, Department of CSE, koneru lakshmaiah Educational Foundation, Vaddeswaram, AP,India.*
ORCID ID : 0009-0008-0679-9403
[22]*Professor, Department of CSE, koneru lakshmaiah Educational Foundation, Vaddeswaram, AP,India.*
ORCID ID : 0009-0009-6373-4769
** Corresponding Author Email: bgvthm38@gmail.com*

infrastructure and sensor locations. To prevent these attacks, various techniques have already been developed to ensure that the wireless nodes are authentic.

The authors in [16] they presented a novel encryption method known as FlexenTech, which utilizes the Internet of Things to improve security and reduce the time it takes to transmit data. The researchers found that this approach can be useful in addressing the challenges of wireless sensor networks, especially those that are in remote locations. For instance, by minimizing the number of rounds that are required to encrypt data, this method can help improve the efficiency of the networks. This approach can be particularly beneficial for MWSNs [17], which are typically deployed within remote locations with little human intervention and limited power supplies. According to the study, establishing secure channels for communication is important to ensure that sensitive data is protected.

Due to the increasing number of applications and the complexity of data security, it is important that the information that is collected and stored in these systems is protected. This is especially true for medical information. Maintaining the freshness and integrity of data is also important to ensure that the responses and outcomes of medical services are correct and timely [18]. Securing medical wearable technologies (MWSNs) is a must as they directly correlate with the privacy and medical condition of patients. The design of an efficient and secure system for MWSNs involves meeting various security requirements. In addition to that, the systems' security mechanisms should be optimized in order to minimize their resource consumption.

The design of a system should also be optimized to minimize the energy consumption and processing speed of its sensors. This is because the devices are usually less powerful than those used in other networks. The lack of resources available to the sensor nodes makes it difficult to implement secure cryptographic methods in certain situations [19].

3. Proposed Architecture

The architecture for medical-WSN devices that allow healthcare facilities and other organizations to collect and manage data is presented in this section. The proposed model can efficiently store the collected data. In addition, we have developed a security method that can protect the confidentiality of the information that the nodes collect.

Fig.1 shows the architecture that we utilized to implement the objectives. It is composed of various users, such as patients and healthcare professionals. The system's modules are labelled below.

• The nodes are equipped with sensors that monitor a patient's condition and continuously collect data.

• The data collected by the nodes can be accessed by healthcare professionals through various monitoring applications.

• The security policies of healthcare facilities are maintained by the Healthcare Authority.

• Cloud storage is utilized to store medical data and ensure its security.

The proposed system consists of lightweight sensor nodes that are attached to each patient. These nodes collect various data points, such as heart rate, motion, and physiological signals, and are then forwarded to a gateway for encryption and data aggregation.

Medical professionals and doctors can use monitoring applications to keep track of their patients' health. These applications can be accessed from anywhere. They use a secret key to decrypt the data collected from the cloud. The monitoring applications utilize the RSK for medical data encryption and utilize a Healthcare Authority (AH) system for access privileges.

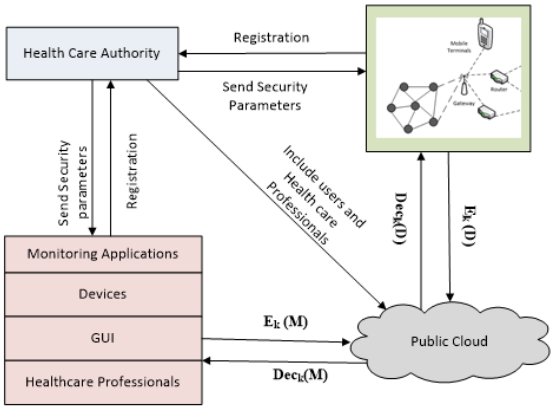

Fig. 1. Proposed Architecture for Medical WSNs.

4. Security Model for Medical WSN

This section focuses on the security model of the proposed architecture and its associated services. The security model comprises three main components: users, healthcare authority (AH), and cloud. The communication between users, AH, and the cloud is safeguarded by implementing the SSL protocol, ensuring data confidentiality and integrity during transmission. However, to securely store data in the cloud, an additional encryption step is performed at the user level. The security model utilizes a public key infrastructure (PKI) to manage the public and private key pairs of each entity involved, enhancing security and authentication within the system.

4.1. Implementation of Security

In the first phase, the Healthcare Authority (AH) creates and utilizes an attribute-based encryption algorithm (ABE)

to generate the public key (PK) and the master key (Ik). The Pk is shared with all users and is used for data encryption and decryption process. The Uk is kept confidential and not disclosed to users. To share the Pk, AH encrypts it using the private key (RK) and sends it to the cloud service providers (C). Users can then verify the authenticity of the private key (Lk) to ensure secure communication.

4.2. Authorization of Healthcare Professionals

Users can join and leave the network of the medical IoT system at any given moment. The healthcare authority (AH) assigns a secret key (Nk) and other access privileges to the user when they want to join the network. These will allow them to decrypt and encrypt data before it is sent to the cloud. The algorithm 1 procedure describes how to validate the user.

Algorithm1: New User Validation

PKI: $P_k \| L_k$

$USR_{Id} \rightarrow$ PKI : USR_{Id}

PKI $\rightarrow$ USR_{ID} : $P_k \| L_k$

$USR_{Id} \rightarrow A_H$: USR_{Id}

$A_H \rightarrow USR_{Id}$: $N_k \| A_P$

A_P : R_{AP} // Read mode

$A_H \rightarrow$ C : [List includes USR_{Id}]

In the first step of the user validation, the public key infrastructure PKI creates the public key Pk and private key Lk to the user, then the CP-ABE algorithm is used by the AH to produce the access policies AP and the secret key Nk to the user. AH requests the C to add the USRID to the List M. In response to the AH request, the cloud includes the USRID along with the corresponding public key (Pk) to the M. Once the communication between the HA and user gateway is established, the user is provided with the secret key (Nk), access privileges (AP), and private key (Lk). These credentials are necessary for the user to securely encrypt, decrypt, and access the relevant data within the system.

The security requirements for patients and healthcare professionals vary depending on the system. For instance, patients must encrypt their data before sending it to cloud services, while healthcare professionals need to have both the W and R access capabilities. With different methods, the AH allows both patients and healthcare workers to access the system. The privileges granted to healthcare professionals are divided into two components. One of these is to protect write mode operations, while the other is to encrypt medical data. Algorithm 2 explains how to authorize and authenticate them.

Algorithm2: Health care professionals Authorization

PKI: $P_k \| L_k$

$H_P \rightarrow$ PKI : USR_{Id}

PKI $\rightarrow$ H_P : $P_k \| L_k$

$H_P \rightarrow A_H$: H_P

$A_H \rightarrow H_P$: $N_k \| A_P$

A_P : $R_{AP} \| W_{AP}$// Read and write mode

$A_H \rightarrow$ C : [List includes H_p]

4.3. Health Care Data management

The health information collected by the sensor nodes is transmitted to the gateway G in an ongoing manner. Algorithm 3 depicts the process of the gateway receiving the sensed information. Then gateway G ciphers the sensor information I and hash value H using the Rsk. Furthermore, G incorporates the access privileges (Ap) into the encrypted RSk. Finally, G forwards the encrypted health information, represented as {USRId, Ek {RSk, Ap}, Ek (I+H)RSk}, to the cloud C. The users can decrypt the data after the gateway has sent encrypted information to the C. They need to first submit the secret key Nk. After that, they can perform an additional step to verify the RSk using the CP-ABE algorithm. After decrypting the data, the user must verify its integrity. If there are any discrepancies, they should send it to the AH.

To ensure data security, the gateway employs a symmetric key encryption method to generate the randomly generated symmetric key (RSK). Additionally, the gateway stores the hash value of the RSk. The SHA-256 hash function is utilized in this process, as it offers stronger security compared to the less secure MD5 method. Table 1 outlines the advantages of using the SHA-256 hash function for this encryption algorithm.

Table 1. Units for magnetic properties

Algorithm	Security	Rounds	Output size (bits)	Speed
SHA-256	Low	24	256	High
MD5	High	64	128	Low

Algorithm 3: Health Care Data Management

S-> sensors, G-> Gateway, C-> cloud

S: Generates the Information I

S→G: USRID, I

G: Generates RSk

G: computes the hash value H to the I

G: uses RSk for Ek(I+H)

G: defines Ap as RAP

G→C: {USRId, Ek {RSk, Ap}, Ek (I+H)RSk}

C→S: Reads the information I

4.4. Medical Data Management

The collected medical information MI is composed of reports, prescriptions, and diagnostics made by healthcare professionals. It may be modified by other users. Each file has a password that prevents unauthorized access. If a user has to perform a specific operation on the data, they need to enter the password of that specific file. Algorithm 4 reveals the steps involved in adding medical data by the Hp. Healthcare professionals follow a similar procedure when accessing the data from the cloud. But, before they can access the data, they must first submit the password (PW). After C validating the password, they can access the data.

Algorithm 4: Medical Data Management

Hp-> Health Care Professionals, G-> Gateway, C-> cloud

HP: Generates the medical information MI

HP→G: USRID, MI

G: Generates RSk

G: computes the hash value H to the MI

G: uses RSk for Ek(MI +H)

G: Encrypt (PW)W

G: defines Ap as RAP and WAP

G→C: {USRId, Ek {RSk, Ap}, (PW)c Ek (MI +H)RSk}

C→S: Read and write the information MI

5. Experiment Analysis

The use of Medical WSN involves the deployment of sensor nodes in various locations, such as hospitals, homes, and public areas. These nodes collect information about a user's medical condition, such as their blood pressure and heart rate, at regular intervals. The collected data is sent to the sink nodes, which then forwards it to the gateway. The gateway then splits the data into fragments. The fragments are sent through various routers. They then forwarded to the cloud storage, where they can be accessed by the users with the appropriate permissions. The generation of a symmetric key using the AES-128 algorithm is carried out efficiently and securely. It uses 128 bit blocks instead of 256 and 192 bits. Compared to other algorithms, it takes less time to generate a key with the AES-128 algorithm. It is very strong and can handle different types of data.

The proposed model ensures data authenticity, confidentiality, integrity, and accessibility when accessing the cloud. It utilizes a symmetric key and CP-ABE [22] to encrypt medical files. The CP-ABE algorithm can be used to prevent unauthorized access to the cloud. It utilizes a random secret key to guarantee the confidentiality of the data. This section compares the proposed and the ABE algorithms, considering the different access privileges for medical data. We also simulated the two using the ABE toolkit [23] and OpenSSL's advanced encryption standard.

The performance of the various algorithms for decryption and encryption, including the proposed and ABE algorithms, was analyzed in Fig. 2 and 3. We compared the computation overheads with the attributes of the different access policies. It has been concluded that the proposed method is more efficient when it comes to addressing the needs of medical data. The main difference between the two is that the proposed method uses the AES algorithm for encryption and the CP-ABE for decryption. Algorithm 3 and 4 shows that the proposed algorithm has a lower computation overhead than the ABE framework. It also offers an efficient access mechanism for decryption and encryption operations. The proposed method employs the AES key encryption algorithm and the CP-ABE algorithm for securing medical records. It has been estimated that the proposed algorithm's overhead is between 16% and 22% in encryption, and between 34% and 46% in decryption.

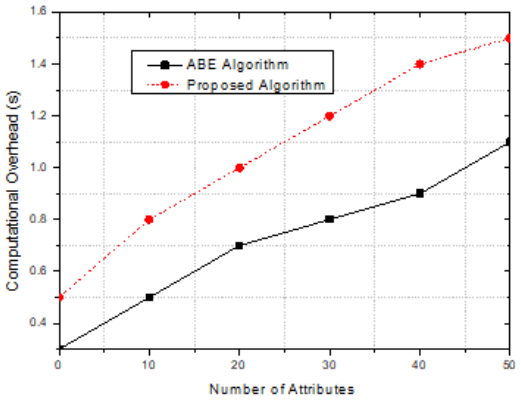

Fig. 2. ABE Vs Proposed algorithm in terms of Encryption

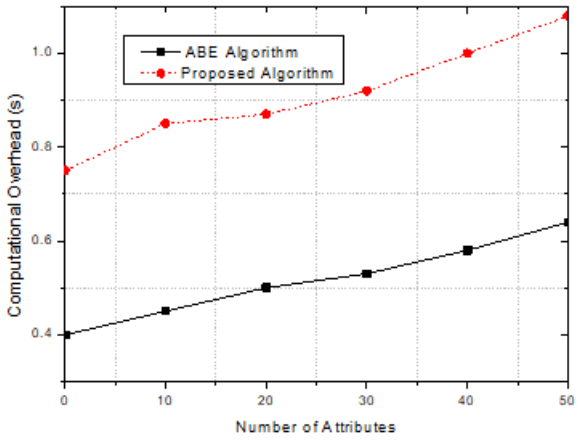

Fig. 3. ABE Vs Proposed algorithm in terms of Decryption

After analyzing the various operations involved in creating, reading, and writing a file, we can then perform a performance evaluation on the three algorithms. The evaluation is carried out according to the number of requests for the given period. The first algorithm is the proposed CP-ABE/AES combination. The second one is the Plutus [20], which has the same key for decryption and encryption. The third one is the SiRiUS [21], which has access control mechanisms and meta-data linked to each file. The user's public key is used for encryption in this algorithm. Figure 4 shows the comparison between the proposed and Plutus algorithms. The SiRiUS has a higher overhead due to the number of operations that it takes in creating and reading a file.

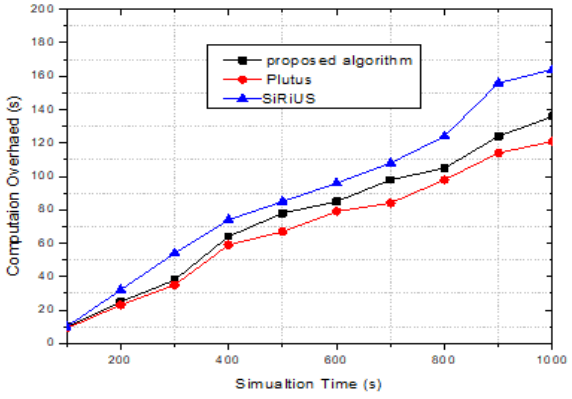

Fig. 4. Computational Overhead of Proposed, Plutus, SiRiUS algorithms with respect to Access Policies

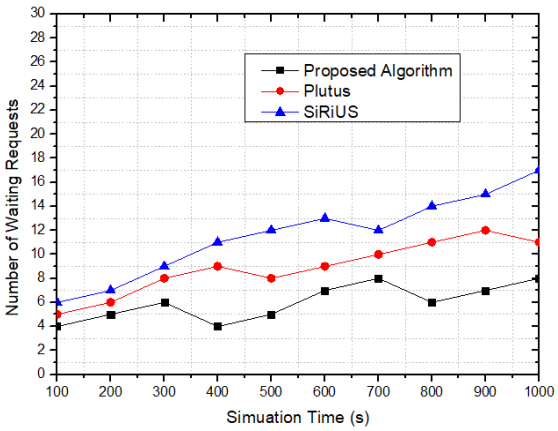

Fig. 5. Computational Overhead of Proposed, Plutus, SiRiUS algorithms with respect to modifications in Access Policies

6. Conclusion

This study introduces a streamlined approach to handle data within the Medical-WSN ecosystem. By leveraging a cloud-based infrastructure, information can be stored and accessed dynamically. The proposed security model is specifically tailored to address the distinct security challenges associated with medical data. It ensures data integrity and confidentiality, offering a robust framework for secure access control. The integration of attributes and symmetric cryptography in the security model enables effective protection of sensitive information. Additionally, the proposed algorithm minimizes computational overhead during encryption and decryption processes. Through experimental analysis, the algorithm demonstrated notable efficiency in terms of security, scalability, and access control, validating its effectiveness for practical implementation.

6.1. Appendix

Appendixes, if needed, appear before the acknowledgment.

6.2. Acknowledgment

The preferred spelling of the word “acknowledgment” in American English is without an “e” after the “g.” Use the singular heading even if you have many acknowledgments. Avoid expressions such as “One of us (S.B.A.) would like to thank ... .” Instead, write “F. A. Author thanks ... .” In most cases, sponsor and financial support acknowledgments are placed in the unnumbered footnote on the first page, not here.

7. References and Footnotes

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Muhajjar, Raad A., Nahla A. Flayh, and Mishall Al-Zubaidie. "A perfect security key management method for hierarchical wireless sensor networks in medical environments." *Electronics* 12, no. 4 (2023): 1011.

[2] Ifzarne, Samir, Imad Hafidi, and Nadia Idrissi. "A Novel Secure Data Aggregation Scheme Based on Semi-Homomorphic Encryption in WSNs." *J. Commun.* 16, no. 8 (2021): 323-330.

[3] Mehmood, Gulzar, Muhammad Sohail Khan, Abdul Waheed, Mahdi Zareei, Muhammad Fayaz, Tariq Sadad, Nazri Kama, and Azri Azmi. "An efficient and secure session key management scheme in wireless sensor network." *Complexity* 2021 (2021): 1-10.

[4] Nidhya, R., Manish Kumar, R. Maheswar, and D. Pavithra. "Security and privacy issues in smart healthcare system using internet of things." *IoT-Enabled Smart Healthcare Systems, Services and Applications* (2022): 63-85.

[5] Al-Zubaidie, Mishall, Zhongwei Zhang, and Ji Zhang. "REISCH: incorporating lightweight and reliable algorithms into healthcare applications of WSNs." *Applied Sciences* 10, no. 6 (2020): 2007.

[6] Chiuchisan I, Dimian M. Internet of Things for e-Health: An approach to medical applications[C]//Computational Intelligence for Multimedia Understanding (IWCIM), 2015 International Workshop on. IEEE, 2015: 1-5.

[7] Zheng X, Chen N, Chen Z, Rong C, Chen G, Guo W, Mobile Cloud based Framework for Remote-Resident Multimedia Discovery and Access, Journal of Internet Technology, 2014, 15(6), 1043-1050.

[8] Whitmore A, Agarwal A, Da Xu L. The Internet of Things: A survey of topics and trends [J]. Information Systems Frontiers, 2015, 17(2): 261-274.

[9] Yang Y. Attribute-based data retrieval with semantic keyword search for e-health cloud [J]. Journal of Cloud Computing, 2015, 4(1): 1.

[10] J. Yang, J. Li, Y. Niu, ”A hybrid solution for privacy preserving medical data sharing in the cloud environment,” Future Generation Computer Systems. 2015, vol. 43-44, pp. 74-86.

[11] A. Abbas, S. Khan, ”A review on the state-of-the-art privacy preserving approaches in e-health clouds,” IEEE Journal of Biomedical Health Informatics, 2014, vol. 18, pp. 1431-1441.

[12] D. Singh, G. Tripathi, and A. J. Jara, ”A survey of Internet-of- Things: Future vision, architecture, challenges and services,” in Proc. IEEE World Forum on Internet of Things, 2014, pp. 287-292.

[13] Bernabe J B, Ramos J L H, Gomez A F S. TACIoT: multidimensional trust-aware access control system for the Internet of Things[J]. Soft Computing, 2016, 20(5): 1763-1779.

[14] Kore, Ashwini, and Shailaja Patil. "Cross layered cryptography based secure routing for IoT-enabled smart healthcare system." *Wireless Networks* (2022): 1-15.

[15] Sharma, Nikhil, Ila Kaushik, Bharat Bhushan, Siddharth Gautam, and Aditya Khamparia. "Applicability of WSN and biometric models in the field of healthcare." In *Deep Learning Strategies for Security Enhancement in Wireless Sensor Networks*, pp. 304-329. IGI Global, 2020.

[16] Bae G, Shin K. An Efficient Hardware Implementation of Lightweight Block Cipher Algorithm CLEFIA for IoT Security Applications[J]. Journal of the Korea Institute of Information and Communication Engineering, 2016, 20(2): 351-358.

[17] Khemissa H, Tandjaoui D. A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things[C]. International Conference on Next Generation Mobile Applications, Services and Technologies. 2015.

[18] Yao X, Chen Z, Tian Y. A lightweight attribute-based encryption scheme for the Internet of Things[J]. Future Generation Computer Systems, 2015, 49(C):104-112.

[19] D.X. Song, D.Wagner, A. Perrig, ”Practical techniques for searches on encrypted data”, in: IEEE Symposium on Security and Privacy, 2000, pp. 44-55.

[20] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu, Plutus: Scalable secure file sharing on untrusted storage, in: Proceedings of the 2nd USENIX Conference on File and Storage Technologies, USENIX Association, Berkeley, CA, USA, 2003, pp. 29–42.

[21] E.-j. Goh, H. Shacham, N. Modadugu, D. Boneh, Sirius: Securing remote untrusted storage, Network and distributed systems security, NDSS’03 (2003) 131—145.

[22] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-Policy Attribute-Based encryption, in: Proceedings of the IEEE Symposium on Security and Privacy, SP ’07, Washington, DC, USA, 2007, pp. 321–334.

[23] B. W. John Bethencourt, Amit Sahai, Cp-abe library, Online at http://acsc.cs.utexas.edu/cpabe/.

[24] Mahajan, R. ., Patil, P. R. ., Potgantwar, A. ., & Bhaladhare, P. R. . (2023). Novel Load Balancing Optimization Algorithm to Improve Quality-of-Service in Cloud Environment. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 57–64. https://doi.org/10.17762/ijritcc.v11i2.6110

[25] Pérez, C., Pérez, L., González, A., Gonzalez, L., & Ólafur, S. Personalized Learning Paths in Engineering Education: A Machine Learning Perspective. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/107

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