*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 11*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

# A Novel Multi Factor Authentication and Encryption Scheme to Secure the IOT Healthcare Data in Cloud

**Aadhinarayanan.N.V, [1*] and Dr.Vijayakumar.P[2]**
[1*]Research Scholar, Department of Computer Science,
Government Arts and Science College (Modakurichi), Bharathiar University,
Coimbatore, Tamil Nadu, India.
[2]Assistant Professor, Department of Computer Science, Bharathiar University,
Coimbatore, Tamil Nadu, India
E-Mail: [1*]nvaadhi@yahoo.com, [2]vijayhodcs@gmail.com

***Abstract:*** The Internet of Things (IoT) application is almost ubiquitous across various human disciplines. The IoT can be integrated into electronic healthcare systems to provide more real-time services on demand, which is extremely useful for patients and clinicians. However, the possibility of encountering untrustworthy information and a possible threat to security is immediately raised. In order to secure the IoT healthcare data in the cloud, the proposed system suggests a novel multi-factor authentication and encryption approach using the Optimal key-based Rivest Shamir Adelman (OKRSA) algorithm. First, the user must register with the trusted authority (TA) of the cloud using the Dual Hash-based Secure Hash Algorithm 512 (DHSHA512). After registration, the patient's data is securely sent to the medical server with the help of the OKRSA algorithm. Finally, the system initiates multi-factor authentication if the user wants to access the files from the cloud medical server. Simulation outcomes proved that the presented scheme offers better security than the previous related schemes.

***Keywords:*** *Internet of Things, Internet of Medical Things, Trusted Authority, Secure data transfer, Hospital cloud server, and Multi factor authentications.*

## 1. INTRODUCTION

The IoT is a new idea that has begun to gain acceptance in modern wireless telecommunications scenarios. They can communicate with one another to achieve common goals by using different addressing systems. The IoT can expedite advancements in applications across a variety of fields, such as automation, smart buildings, industrial automation, medical aids, traffic management, mobile healthcare, and intelligent energy management [1]. Smart medical gadgets in healthcare connect people and innovative items, making life easier and simpler. The Internet of Medical Things (IoMT) is quickly becoming a critical component of healthcare. It offers intelligent healthcare services by gathering various information and delivering it to the cloud [2]. Not only are wearable patient devices vulnerable to security issues, but the gathered and sent data are also vulnerable during communication; thus, the entire ecosystem must be protected against internal and external threats [3]. The current method has many irregularities in securing patient data. It takes up more memory space to store medical data, which could be more efficient. The cloud provides excellent security to protect patient data [4]. The cloud provides many services, such as data storage, data management, databases, software, and networking. Cloud users can access these services and data via the Internet [5]. However, once a substantial security measure is implemented, medical data exchange from one node or user to another or across the cloud platform is hazardous [6]. Using authentication procedures to ensure data secrecy is a frequent solution [7].

Authentication is essential before real-time data transmission between healthcare users since it lowers harmful errors and inaccuracies in specifying pharmaceutical dosages, timings, and techniques. As a result, authentication protocols have emerged as a fundamental necessity for real-time healthcare systems [8]. Authentication protocols are classified into two types: identity-based authentication and message-based authentication. Nevertheless, since many IoT sensors lack the memory and CPU power needed for conventional authentication protocols, there is an increase towards lightweight authentication protocols [9]. As a result, the suggested system employs efficient hashing-based authentication mechanisms to offer safe access to or download from the hospital cloud server. Furthermore, various symmetric and asymmetric algorithms can securely send data to the cloud [10]. Symmetric essential methods are quick but have various drawbacks, including difficulties in distributing keys, needing more scalability, and providing secrecy. On the other hand, asymmetric key techniques do not suffer such issues, although being considerably slower [11]. As a result, the suggested system employs the optimal key-

based RSA method to make the system speedier and to select the best key for safe data transmission to the healthcare cloud server. The contributions of the proposed research framework are explained as follows:

- To present the DHSHA512 algorithm to generate the hash value for the user details and to authenticate the users at the time of login.
- To propose an OKRSA algorithm to transmit medical data to a medical cloud server securely.
- To employ multi-factor authentication mechanisms to protect cloud-stored data from malicious users.
- To perform a comprehensive evaluation to prove the proposed work's efficiency with the existing methods.

The remaining phases of the manuscript are described as follows: Section 2 presents the survey of recent authentication and encryption methodologies for secure IoT-based healthcare systems. Section 3 presents a detailed explanation of the proposed research model. The simulation analysis of the proposed and existing methodologies is given in section 4. Finally, the conclusion of the suggested model is given in section 5.

## 2. RELATED WORK

Here, we discuss some authentication protocols and encryption methods previously presented in the literature.

**Mehedi Masud *et al.* [12]** presented a secure authentication scheme for IoT-based healthcare systems. The healthcare professional (doctor) initially registered with the gateway to get the patient's health information. At the same time, the sensor devices were registered with the gateway to send their patient's information to the doctors. The secret session key was generated between the sender and receiver to authenticate themselves in data transmission. Once both sender and receiver were authenticated, the data was transmitted from one end to another. The system achieved a communication cost of 2042 bits which was lower than the conventional authentication schemes. **Maryam Nasr Esfahani *et al.*** [13] suggested an end-to-end security framework for IoT based healthcare environment. Initially, the key distribution centre registered gateways, application users, and application providers (APs), and the network manager registered sensor nodes in the network. The gateways received the healthcare information from the sensor devices once they were authenticated and sent the received information to the APs. Finally, the AUs got the patient's data from the APs once they were authenticated in the network. The method was superior to previous related schemes by achieving a minimal computation overhead of 116 bits. **Daya Sagar Gupta *et al.* [14]** presented a secure authentication and access control framework for IoT-based healthcare systems. Initially, the medical server initiated the setup phase for the user data access in the network. The registration of the data user was done at the medical server by providing their user's name, password and smart card. After registration, verification was done on the medical server to permit the user to access data. The method offered better performance regarding transmission, computation overhead and key storage overheads.

**Wenchao Li *et al.* [15]** suggested an equality test and proxy re-encryption scheme for secure data transmission in IoT-assisted healthcare environments. Initially, the user received the key from a TA and encrypted the data using the public key. The encrypted data was sent to the cloud server for secure data storage. The encrypted data was searched at the proxy by generating the trapdoor. Finally, the decryption of the encrypted data was done to get the original data of the user. The method attained lower communication and computational costs than the conventional schemes. **Mikail Mohammed Salim *et al.* [16]** presented a homomorphic encryption scheme to secure the network of the IoMT. Initially, the nodes in the network were clustered, and the clustered data was sent to the base station. Then the received data was encrypted using HE to secure the network's various attacks and intruders. The data was decrypted and sent back to the user for healthcare monitoring. The system achieved better security outcomes than the existing schemes.

Most of the works mentioned above-used single-factor authentication schemes for securing healthcare platforms, and its security mainly depends only on user name, password, and PIN. However, third parties can identify it quickly when sharing these details via the unsecured channel. As a result, the suggested system employs a multi-factor authentication approach, which tends to be more secure than a single factor since it is harder for an attacker to steal multiple factors. In addition, the secure transmission of healthcare data to the cloud is also a more challenging issue because the transmission data holds the patient's sensitive information. Sometimes, third parties collapse the data during transmission. Employing effective encryption mechanisms protects the data from theft. However, most of the existing works use symmetric encryption techniques, but the message's origin and validity cannot be guaranteed here. Hence some existing works use asymmetric encryption techniques, but the key generation in asymmetric encryption is complex. Because asymmetric encryptions use random keys to encrypt and decrypt the data, these random key generation increases the complexity of the computational

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 11*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

process. So, the proposed system uses an OKRSA to securely transmit the data to the cloud.

## 3. PROPOSED METHODOLOGY

This paper proposes a multi-factor authentication and lightweight encryption scheme to transmit and store medical IoT data securely. The proposed system mainly consists of three phases: registrations, secure data transfer, and authentication. Initially, the user registers to the TA of the cloud to securely access the system by using the DHSHA512 algorithm. Then the patient IoT is securely transmitted to the hospital cloud server using the OKRSA algorithm. Finally, the system implements the multi-factor authentication scheme if they want to read and download the file from the cloud server. The working process of the proposed work is shown in Figure 2.

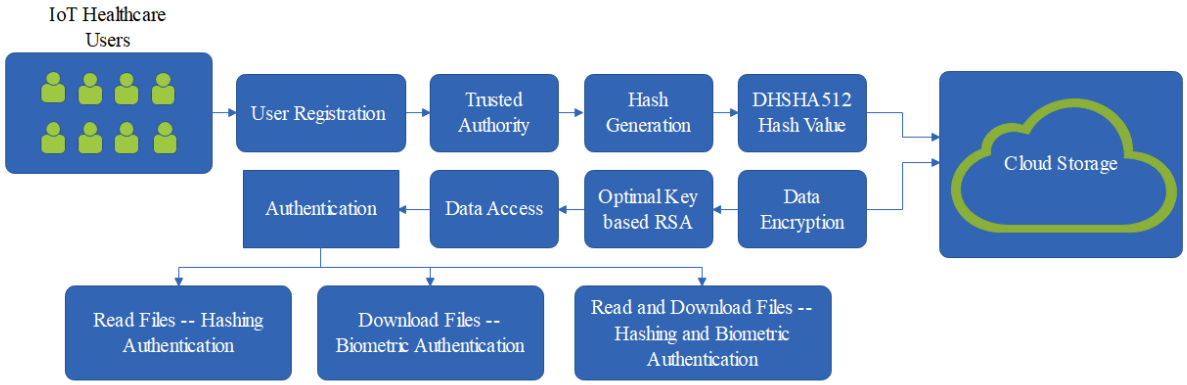



Figure 2: Proposed model's workflow

### 3.1 Registration

With the help of a medical device, the user (doctor, nurse or patient) gets registration by the TA of the cloud via a secure channel to access the system. To register with the TA of the cloud, the information that needs to be provided by the user is name $(U_{name})$, user ID $(U_{ID})$, password $(U_{PW})$, gender $(U_{Gender})$, birth date $(U_{DOB})$, home address $(U_{HADD})$, and biometric samples $(U_{BSAM})$.After that, TA generates the hash value for the user-provided details with the help of DHSHA512 and stores these hash values on the cloud server for authentication purposes. The SHA 512 is a hash function-based method developed by Ron Rivest. The hash function in this method acts on an arbitrary-length message and returns a fixed-length output known as the 'hash value' or message digest 512-bit size and 1024-bit block length. It provides better security to the proposed system during authentication time. Although it provided additional security to the proposed work, the system performed a double hash, which improved the system. Thus, it is called DHSHA512. The padding function is used to append a specified number of bits to the original message (user ID, password, and date of birth) to increase its length, which should be 128 bits less than an exact multiple of 1024. After this, the size of the original message given to the algorithm is appended. After that hash value of the original message is calculated by using the following equation.

$$\overline{V}''_{val} = SHA\_512\left(U_{ID} \| U_{PW} \| U_{DOB}\right) \tag{1}$$

Where, $\overline{V}''_{val}$ indicates the hash value for the user-provided details. These hash values are hashed again using the same process to provide additional security to the system. This is expressed as follows:

$$\overline{FH}''_{val} = SHA\_512\ \left(\overline{V}''_{val}\right) \tag{2}$$

Thus, the final hash values for the user-provided details are stored in the cloud server for authentication purposes.

### 3.2 Secure Data Transmission

After registration, the patient IoT data is securely transmitted to the hospital cloud server using an OKRSA. The RSA is the most widely utilized asymmetric cryptography mechanism based on mathematical facts. It is easy to get and multiply huge prime numbers together. It uses public and private keys to perform encryption and decryption. Its asymmetric behaviour enables secure communication between the sender and receiver. The different key sizes of RSA include 512 bits,

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 11*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

1024 bits, 2048 bits, and 3072 bits. However, a poor choice of keys for encryption and decryption can compromise the RSA cryptosystem's security. So, the proposed system uses a Modified Reptile Search Optimization (MRESO) algorithm for optimal key generation. It extends the security level and makes the computation procedure very easy. Thus, this optimal key selection process in the conventional RSA scheme is termed the OKRSA algorithm. The OKRSA algorithm involves three steps such as key generation, encryption, and decryption, which are deeply explained as follows:

***Step 1:** Key generation*

Select two different large arbitrary prime numbers $\overline{A}$ and $\overline{B}$ . Then calculate $\overline{M} = \overline{A} \,.\, \overline{B}$ , where, $\overline{M}$ is used as the modulus for private and public keys. Next, estimate the Euler totient function ($\varphi^*$ ) of $\overline{M}$ using equation (3).

$$\varphi^* \left(\overline{M}\right) = \left(\overline{A} - 1\right) * \left(\overline{B} - 1\right) \tag{3}$$

After that public key is randomly generated between the range of 1 to $\varphi^* \left(\overline{M}\right)$, but these randomly generated keys make the computation of the system was slower and if they are not chosen optimally, they generate infinity values. So, the proposed system uses the MRESO algorithm to select the keys optimally. Reptile search optimization (RESO) is inspired by crocodiles' natural surroundings, hunting habits, and social behaviour. Crocodile behaviour is divided into two phases: exploration (global) and exploitation (local), which involve encircling and hunting the prey. RESO is competitive compared to other algorithms but has limited population diversity, uneven exploration and exploitation, and a proclivity to get stuck into local optima. A highly disruptive polynomial mutation (HDPM) increases population diversity to address these problems. Second, a Constant constriction factor (CCF) is proposed to balance the exploration of reptiles. These two modifications in the conventional RESO algorithm are termed MRESO. In MRESO, the initial populations of reptiles are initialized using the HDPM strategy, which enhances the diversity of the population. This is mathematically expressed as follows:

$$\overline{\mathrm{H}}_{(p,q)} = \overline{\mathrm{H}} + \rho_m \,.\, \left(UB_{val} - LB_{val}\right) \tag{4}$$

Where, $\overline{\mathrm{H}}_{(p,q)}$ refers to the decision variable of the $p^{-th}$ solution at the $q^{-th}$ position, $\overline{\mathrm{H}}$ indicates the parent of reptiles, $UB_{val}$ and $LB_{val}$ signifies the upper and lower boundaries of the search space. The coefficient $\rho_m$ is calculated as follows:

$$\rho_m = \frac{\overline{\mathrm{H}} - LB_{val}}{UB_{val} - LB_{val}} \tag{5}$$

Once populations of reptiles are initialized, then compute the individuals' fitness. The fitness function is evaluated for every individual, improving the proposed work's security. After computing the fitness, the global searching process is done, in which crocodiles carry out high and sprawl walks. The process is often limited to the first half of the total iteration. Equation (6) simulates the exploration process of the crocodile and is shown below:

$$\overline{\mathrm{H}}_{(p,q)}\left(\lambda+1\right) = \begin{cases} \overline{\mathrm{H}}_q^{best}\left(\lambda\right) - \kappa_{p,q}\left(\lambda\right) \times \delta - \overline{\mathrm{Y}}_{p,q}\left(\lambda\right) \times RN_{num}, \\ \overline{\mathrm{H}}_q^{best}\left(\lambda\right) \times \overline{\mathrm{H}}_{\tilde{R}_1,q}\left(\lambda\right) \times S_{evs}\left(\lambda\right) \times RN_{num}, \end{cases} \tag{6}$$

Where, $\overline{\mathrm{H}}_q^{best}\left(\lambda\right)$ signifies the best solution obtained by an algorithm at $q^{-th}$ position and iteration $\lambda$ , $\delta$ controls the high walking strategies' exploration ability and this value is set to 0.1, $\kappa_{p,q}\left(\lambda\right)$ refers to the hunting parameter which is calculated using equation (7), $\overline{\mathrm{Y}}_{p,q}$ indicates the reduce function that is used to compact and optimize search space which is calculated by using equation (9), $S_{evs}$ indicates the evolutionary sense probability parameter, which is evaluated by using equation (10), and $RN_{num}$ signifies the random number which is generated between 0 to 1.

$$\kappa_{p,q}\left(\lambda\right) = \overline{\mathrm{H}}_q^{best}\left(\lambda\right) \times \overline{C}_{p,q} \tag{7}$$

$$\overline{C}_{p,q} = \chi + \frac{\overline{\mathrm{H}}_{p,q} - Avg\left(\overline{\mathrm{H}}_p\right)}{\overline{\mathrm{H}}_q^{best} \times \left(UB_{val} - LB_{val}\right) + \tau} \tag{8}$$

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 11*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

$$\overline{\mathrm{Y}}_{p,q} = \frac{\overline{\mathrm{H}}_q^{best} - \overline{\mathrm{H}}_{\tilde{R}_2,q}}{\overline{\mathrm{H}}_q^{best} + \tau} \tag{9}$$

$$S_{evs} = 2 \times \tilde{R}_3 \times \left(1 - 1/\lambda\right) \tag{10}$$

Where, $\overline{C}_{p,q}$ indicates the percentage difference between the decision variable at the same positions of the current solution $\overline{\mathrm{H}}_p$ and decision variable at the $q^{-th}$ position of the best solution $\overline{\mathrm{H}}^{best}$, $\chi$ is a constant value (0.1 in the proposed system) that controls the exploration's speed, $\tau$ indicates a minimum value but not 0, and $\tilde{R}_1$, $\tilde{R}_2$, and $\tilde{R}_3$ denotes the arbitrary numbers that lie between [-1, 1]. The RESO then designs the hunting phase to use the present search areas to find the ideal solutions using hunting coordination and cooperation, as illustrated in equation (11).

$$\overline{\mathrm{H}}_{(p,q)}(\lambda+1) = \begin{cases} \overline{\mathrm{H}}_q^{best}(\lambda) \times \overline{C}_{p,q} \times RN_{mum} \times M_{ft}, \\ \overline{\mathrm{H}}_q^{best}(\lambda) - \kappa_{p,q}(\lambda) \times \tau - \overline{\mathrm{Y}}_{p,q} \times RN_{mum} \times \end{cases} \tag{11}$$

Where, $M_{ft}$ refers to the constant constriction factor, which guarantees the RESO convergence to global optima. It is a function that is convex in nature and so global search is possible. This is mathematically expressed as follows:

$$M_{ft} = \frac{2.43 + \cos\left(2\pi / Tot\_Iter \times \left(\lambda - Tot\_Iter/2\right)\right)}{4} \tag{12}$$

Where, $Tot\_Iter$ refers to the total number of iterations. The iteration process ends if the optimal solution (optimal key) is obtained. Otherwise, the iteration process is repeated until the best optimal solutions are obtained. Once the optimal public key is generated, compute the private key using equation (13).

$$\overline{PR}_{key} = \left(\overline{PU}^*\right)^{-1} \bmod \varphi^*\left(\overline{M}\right) \tag{13}$$

Where, $\overline{PR}_{key}$ refers to the private key and $\overline{PU}^*$ denotes the optimal public key generated by the MRESO algorithm.

***Step 2:** Encryption*

Once the key generation process is completed and then the data is encrypted using the public key, which is the input data is converted into ciphertext and securely transmitted to the hospital cloud server. The ciphertext is computed as follows:

$$Ci\_Text = \left(OD_m\right)^{\overline{PU}^*} \bmod \overline{M} \tag{14}$$

Where, $OD_m$ refers to the input data to be transmitted to the cloud.

***Step 3:** Decryption*

The authentication process is given in section 3.3. It is the converse process of encryption algorithm where the principle of changing encrypted data to original data by the private key. Only authenticated users are allowed to decrypt the original data. The following equation is used to decrypt the original data from the cloud.

$$OD_m = \left(Ci\_Text\right)^{\overline{PR}_{key}} \bmod \overline{M} \tag{15}$$

### 3.3 Authentication

One of the most crucial needs in any IoT-based healthcare system is to deal with impersonation threats. Authentication aids in confirming their identities to one another in an unsecured channel. In this proposed work, multi-factor authentication happens to access the data from the hospital cloud server securely, and this is explained as follows:

***Step 1:*** The first level of user authentication is performed if the user wants to read the file from the cloud server. The user wants to send a read request to the cloud server and then share their username, password, and dob with the TA. The TA then computes the hash value of the user-provided details using the DHSHA512 algorithm and checks the estimated hash value with the already stored one in the cloud. If both matches, the access for the user is granted to read the data from the cloud.

***Step 2:*** The second level of user authentication is performed if the user wants to download the file from the cloud server. The user wants to send a download data request to the cloud server and then share their biometrics record with the TA. The TA then checks the entered biometric data with the already stored one (during registration) in the cloud. If both matches, the user can download the data from the cloud, and the key is also provided to decrypt the data.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 11*
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 November 2023*

***Step 3:*** The final level of user authentication is performed if the user wants to perform dual action, i.e., read and download the data from the cloud. The user wants to send data read and download requests to the cloud server and then share details such as username, password, dob and biometric records to the TA. The TA then checks the entered data with the already stored one (during registration) in the cloud. If both matches, the access for the user is granted to read and download the data from the cloud. Otherwise, the permission is not granted to the users.

## 4. RESULTS AND DISCUSSION

This section analyzes the outcomes of the proposed system with the existing systems regarding some security metrics. The proposed system is implemented in the operating platform of the NS3 network simulator. The simulation is done within a range of 1000 × 1000 m, and the number of IoT medical sensor nodes considered is 20 to 100 respectively. The following section analyses how well the proposed work was performed.

### 4.1 Performance Analysis

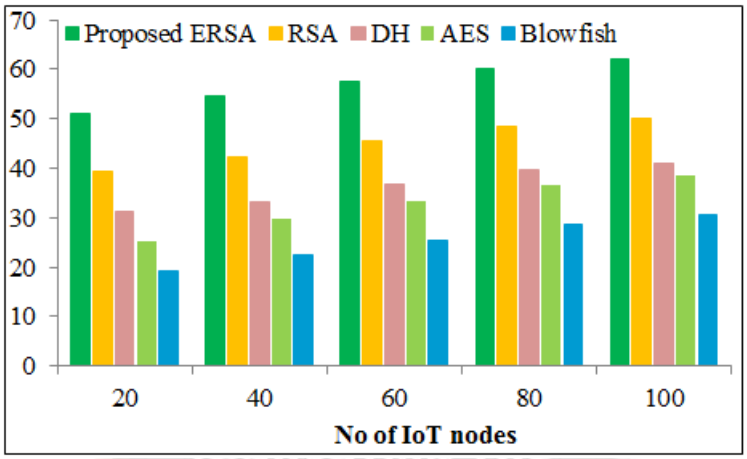
This section investigates the outcomes of the proposed OKRSA against the conventional RSA, Diffie Hellman (DH), Advanced Encryption Standard (AES), and Blowfish algorithm concerning the encryption time (ET) and decryption time (DT) for the number of IoT nodes 20 to 100.

Table 1: ET and DT analysis

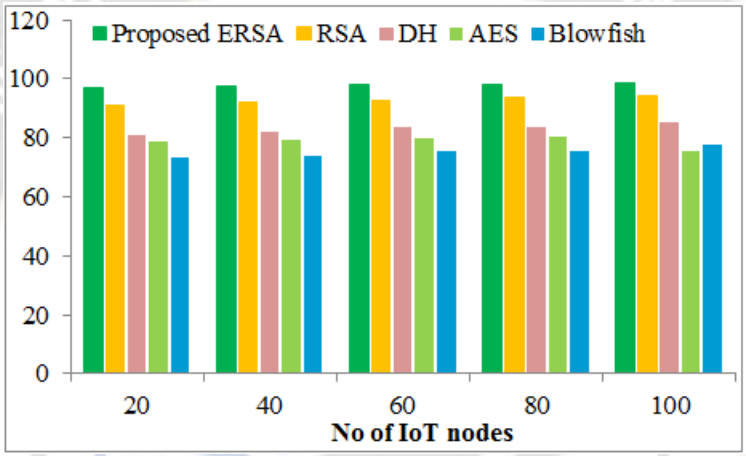
| Metrics | No of IoT nodes | Proposed OKRSA | RSA | DH | AES | Blowfish |
|---|---|---|---|---|---|---|
| ET $(\mu s)$ | 20 | 1.02 | 1.25 | 1.39 | 1.53 | 1.72 |
| | 40 | 1.34 | 1.46 | 1.72 | 1.93 | 2.03 |
| | 60 | 1.58 | 1.65 | 1.98 | 2.14 | 2.21 |
| | 80 | 1.74 | 1.87 | 2.11 | 2.31 | 2.49 |
| | 100 | 1.95 | 2.01 | 2.32 | 2.56 | 2.68 |
| DT $(\mu s)$ | 20 | 0.98 | 1.19 | 1.31 | 1.42 | 1.71 |
| | 40 | 1.26 | 1.38 | 1.65 | 1.85 | 1.94 |
| | 60 | 1.51 | 1.59 | 1.89 | 2.04 | 2.09 |
| | 80 | 1.68 | 1.81 | 2.04 | 2.18 | 2.39 |
| | 100 | 1.88 | 1.92 | 2.21 | 2.42 | 2.57 |

Table 1 illustrates the outcomes of the proposed OKRSA and conventional methods regarding encryption and DT. The outcomes are tabulated by varying the number of medical sensor nodes from 20 to 100. For 20 sensor node, the proposed one takes ET and DT of 1.02 $\mu s$ and 0.98 $\mu s$, but the conventional RSA, DH, AES, and Blowfish takes the ET of 1.25 $\mu s$, 1.39 $\mu s$, 1.53 $\mu s$, and 1.72 $\mu s$ and DT of 1.19 $\mu s$, 1.31 $\mu s$, 1.42 $\mu s$, and 1.71 $\mu s$, respectively, which are higher than the proposed one. Similarly, for the remaining nodes, the proposed one takes minimal time to encrypt and decrypt the data. From the table, it concluded that the proposed one achieves more excellent performance than the conventional methods. Figure 2 shows the outcomes of the encryption models regarding (a) throughput and (b) reliability. Throughput represents the number of messages effectively delivered to the destination in a particular amount of time, and reliability is also an important metric showing the system's security level. First, considering the throughput metric, the proposed one has a throughput of 51.12kbps for 20 sensor nodes, but the existing RSA, DH, AES, and Blowfish attain the throughput of 39.23kbps, 31.12kpbs, 25.12kbps, and 19.35kbps, which are lower than the proposed scheme. Also, for the remaining no of nodes, 40 to 100, the proposed one achieves higher throughput compared to the conventional methods. This shows the effectiveness of the proposed system in data transmission. Next, concerning the reliability metric, the proposed one has the reliability of 97.03%, 97.56%, 97.9%, 98.12%, and 98.56% for the number of IoT nodes 20 to 100, respectively, which is a high-reliability rate than the conventional methodologies. This shows the higher-level security achievement of the proposed system over others in cloud data storage.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 11*
***Article Received:*** *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 November 2023*




**(a)**




**(b)**

Figure 2: Throughput and reliability analysis

## 5. CONCLUSION

In this paper, a novel multi-factor authentication and encryption scheme was developed to secure IoT-based healthcare systems. The proposed work comprised three phases: registration, secure data transmission, and authentication. The outcomes of the proposed OKRSA are compared with the existing RSA, DH, AES, and Blowfish encryption algorithms regarding ET, DT, throughput, and reliability metrics by varying the IoT medical sensors from 20 to 100. The simulations are carried out to analyze the efficiency of the proposed model over other existing schemes. For 20 nodes, the proposed one attains ET, DT, throughput, and reliability of 1.02 $\mu s$ , 0.98 $\mu s$ , 51.12kpbs, and 97.03%, respectively, which are better than the traditional methods. Likewise, the proposed one produces superior results for the remaining number of nodes compared to the existing encryption schemes. Thus, the experimental and simulation analysis showed that the proposed system is efficient, secure, and more practical than the existing encryption schemes. The work will be extended in the future by including blockchain mechanisms and another advanced cryptographic model in providing secure data access and storage in IoT-based healthcare systems.

## REFERENCES

[1] Almalki, F. A., & Soufiene, B. O. (2021). EPPDA: an efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. *Wireless Communications and Mobile Computing*, *2021*, 1-18.

[2] Ullah, A., Azeem, M., Ashraf, H., Alaboudi, A. A., Humayun, M., & Jhanjhi, N. Z. (2021). Secure healthcare data aggregation and transmission in IoT—A survey. *IEEE Access*, *9*, 16849-16865.

[3] Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy

decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors*, *22*(4), 1448.

[4] Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocessors and Microsystems*, *80*, 103301.

[5] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. *Journal of medicine and life*, *14*(4), 448.

[6] Denis, R., & Madhubala, P. (2021). Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems. *Multimedia Tools and Applications*, *80*, 21165-21202.

[7] Azrour, M., Mabrouki, J., & Chaganti, R. (2021). New efficient and secured authentication protocol for remote healthcare systems in cloud-iot. *Security and Communication Networks*, *2021*, 1-12.

[8] Dewangan, K., Mishra, M., & Dewangan, N. K. (2021). A review: A new authentication protocol for real-time healthcare monitoring systems. *Irish Journal of Medical Science (1971-)*, *190*, 927-932.

[9] Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2022). A survey on security threats and countermeasures in the internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies*, *33*(6), e4049.

[10] Rajasekar, V., Premalatha, J., Sathya, K., & Saračević, M. (2021). Secure remote user authentication scheme on health care, IoT and cloud applications: a multilayer systematic survey. *Acta Polytechnica Hungarica*, *18*(3), 87-106.

[11] Malmurugan, N., Nelson, S. C., Altuwairiqi, M., Alyami, H., Gangodkar, D., Abdul Zahra, M. M., & Asakipaam, S. A. (2022). Hybrid Encryption Method for Health Monitoring Systems Based on Machine Learning. *Computational Intelligence and Neuroscience*, *2022*.

[12] Masud, M., Gaba, G. S., Choudhary, K., Hossain, M. S., Alhamid, M. F., & Muhammad, G. (2021). Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet of Things Journal*, *9*(4), 2649-2656.

[13] Nasr Esfahani, M., Shahgholi Ghahfarokhi, B., & Etemadi Borujeni, S. (2021). End-to-end privacy preserving scheme for IoT-based healthcare systems. *Wireless Networks*, *27*(6), 4009-4037.

[14] Gupta, D. S., Mazumdar, N., Nag, A., & Singh, J. P. (2023). Secure data authentication and access control protocol for industrial healthcare systems. *Journal of Ambient Intelligence and Humanized Computing*, 1-12.

[15] Li, W., Jin, C., Kumari, S., Xiong, H., & Kumar, S. (2022). Proxy re-encryption with equality test for secure data sharing in Internet of Things-based healthcare systems. *Transactions on Emerging Telecommunications Technologies*, *33*(10), e3986.

[16] Salim, M. M., Kim, I., Doniyor, U., Lee, C., & Park, J. H. (2021). Homomorphic encryption-based privacy-preservation for iomt. *Applied Sciences*, *11*(18), 8757.