European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 08, Issue 01, 2021

Securing Medical Data using Extended Role Based Access Control Model and Twofish Algorithms on Cloud Platform

T.Jayasankar*[1], R.M.Bhavadharini[2], N.R.Nagarajan[3], G.Mani[4], S. Ramesh[5]

[1]*Assistant Professor (Sr.Gr), Department of Electronics and Communication Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, Tamilnadu, India. Email: jayasankar27681@gmail.com*

[2]*Associate Professor, Department of Computer Science and Engineering, Easwari Engineering College, Chennai, India. Email:rmbhavadharini@gmail.com*

[3]*Assistant Professor, Department of Electronics and Communication Engineering, K.Ramakrishnan College of Engineering, , Tiruchirappalli, Tamilnadu, India. Email: naguube@gmail.com*

[4]*Assistant Professor (Sr.Gr), Department of Computer Science and Engineering, University College of Engineering, Arni, Tamilnadu, India Email:gmani1879@gmail.com*

[5]*Assistant Professor, Department of Computer Science and Engineering, Krishnasamy College of Engineering & Technology, Cuddalore, Tamilnadu, India. Email:swami.itraj@gmail.com*

Abstract

A great deal of data is generated and collected by devices connected to healthcare systems on the Internet of Things (IoT). This data is distributed in real time, is unstructured in nature, and it is also a big problem to store and process in IoT applications. Since cloud computing is so common, many healthcare providers store these EHRs in cloud systems. Unauthorized access to these medical records is nevertheless still an issue. In order to avoid unauthorised access to this medical data in the public cloud networks, many access management models, along with cryptographic techniques have been used. This article proposes Enhanced Role Based Access Control (ERBAC) and Twofish algorithm to protect IoT health data in health systems from a public cloud storage perspective. The authors believe that the proposed system will significantly aid in the efficient storage of medical data in IoT applications and will provide secure storage of medical data in the cloud based on these role-based access policies. Additionally, a clustering strategy is introduced into the paper to reduce the waiting time for retrieving relevant medical data. The clustering of clinical data is the rational underlying approach for discovering secret examples from a wide variety of clinical data. Clinicians have rendered a professional decision on the disease probability using these cases. Clustering categories, the data set of separate collections based on comparability of information in the database is larger than other collections.Thus, this work proposes a clustering method that uses particle swarm optimization (PSO) with a genetic algorithm (GA) and proposes another clustering strategy called clustering calculation, based on the calculation of the advance of a swarm of molecules. It uses worldwide improvements in PSO calculation to fill the lack of the grouping strategy.

Keywords: Internet of Things; Health; Access control; Particle Swarm Optimization; Medical Data Clustering; Data Security; Twofish.

Introduction

We know that although the digital revolution has begun previously in the medical industry, it has been slowly progressing relative to other areas[1]. Medical care has become one of the focal points of personal, social and even national concern with the exponential growth of science, technology and economy. The conventional medicine paradigm has challenges such as trouble seeing a specialist, costly care, and the occlusion. However the IoT application area was interested in all dimensions with the systematic implementation of the Internet of Things definition in 1999[3],[4] in the new age of the Internet of All (IoE)[5]. In the field of medicine, the Internet of Medical Stuff (IoMT) reflects the concentrated incarnation of IoT technology and is also the centre of the modern medical revolution. The digital processing of medical records is carried out by implementation of IoT technology in the medical sector[6], so that medical personnel do not spend more time on documenting and arranging a wide variety of burdensome health information, but instead on patients as a centre to provide better healthcare services. In comparison, in combination with cell endpoints, network connectivity and other applications, IoMT is used to achieve connectivity with patients, medical staff, medical institutions and medical devices in order to achieve digitisation and automated interaction, such as IoT technology (radio frequency recognition, sensor technologies and positioning technology) [7]. The IoMT includes every aspect, including identity recognition, tracking of critical signs, remote monitoring, prescription medicines, waste and monitoring of appliances.

While IoT technology application will lead to the intelligent medical care of patients and the intelligent management of things in hospitals in the medical sector, various medical institutions are relatively separate, so resource sharing is very difficult to achieve[8]. The cloud-based IoMT offers efficient IT services and dramatically lowers costs for medication. It is not only able to reach the mass storage of medical records, it will carry out the distribution and efficiency of medical knowledge across the cloud network. However, relying solely on cloud storage consumes immense network communication capital, which can pose a risk to patients' lives[9-10]. Cloud computing provides the potential to handle data sinks, allowing data collection nearer to the source than external data or cloud that can reduce the delay and allow medical data readily and quickly analysed and analysed. A common Role Based Access Management and two-fish algorithm model for maintaining protection in data storage in public clouds was addressed, where authenticated users can access data only in positions with allocated allowances, and limit unknown users to data access by adding variable limits. In addition, the paper utilises the hybrid algorithms clustering technique clearly explained in the section proposed.

The paper is organized as follows: Section 2 presents the literature review that explains drawbacks of existing techniques. Section 3 discuss the role of IoT in Healthcare system, where proposed methodology is given in Section 4. The results of the proposed methodology with existing techniques is provided in Section 5. Finally, the conclusion of the research study is described in Section 6.

2. Literature Review

The app validation, one-factor authentication, multi-factor authentication and static authentication have also become conventional identity authentication systems for hardware certification. Subsequently, researchers suggested new ones based on current authentication schemes.

Xu et al. proposed a stable and reliable two-factor shared authentication and the main cryptosystem protocol. [9]. [9]. Subsequently, an elliptical curve-based encryption of the two-factor authentication protocol is often recommended [12,13]. Zhang et al. targeted data source protection certification, frontend blockchain and trustworthy SGX hardware[14] certification. Liu et al. also developed a new bilinear pair for the wireless body area network on the elliptical curve. The certificate less signature scheme is not able to survive simulated attack, and the preceding schemes will be carried out on the basis of their own work and an optimised anonymous authentication schemes will be proposed[15].

Renuka introduced a three-factor security authentication method for smart medical care focused on the benefits of USB[16]. Lin et al. said the benefit of blockchain decentralisation reforms conventional authentication. In the case of existing X.509 certificate requirements, but AI-Bassam is unable to sign fine-grained attribute information attribute certificates for user identities only. It is enhanced and the attribute information is validated on the basis of the intelligent contract. If authenticated, the identification attribute of the user identity is still trustworthy and trust is conveyed between the user identity and the user's attribute [17]. Nikolaoet al. used blockchain technologies to secure and model TM device authentication[18]. Nikolao et al. Perera et al. must validate the identities of several participants on the basis of their multi-user identity. This leads to the implementation of a mechanism of defining and checking on the basis of sparse representation [19]. Lin et al. implemented a node-signature (for example to mark book nodes) method that allows signer certificate to easily upgrade the trapdor hash function, without re-signing the node.[20] Lin et al. have developed a new scheme for the transfer of undirected graphs.

It was conveyed to S.Hirani[21] that certain tests were being carried out with encryption AES algorithms quicker and more effectively. When applying transmission data, he discovered that various symmetrical key schemes have a difference in their efficiency. He indicated that AES is best for transmitting data. P. TheRuangchaijatupon [22] reveals that various common symmetrical key algorithms are used to produce energy consumption on different machines. Health records and medical data are increasingly growing in the present population. A powerful management framework was suggested by AnjanaDevi[23] to protect the patient information and report by doctors in clinical laboratories. Anjana Devi is designing labs to build a swift and effective method for the protection of cryptic threats. Using the encryption and decryption algorithm, the proposed method secures the patient data and the patient reports against the cloud stock. For all these procedures, the patient test report and data from the healthcare sector are secured using a two-found algorithm. A broad Aziz Muslim[24] suggested an idea of the two-fish algorithm being applied in a data protection communication network using Chilkat library. They also employed an agile strategy for integrating the applications as fast as possible.

The standard philosophy and technology for authentication is focused largely on the trustworthy process of third parties, where the integrity of third parties is disputed and often

requires several heterogeneous networks, diverse node types and various user nodes in the health care context. Security authentication between nodes and devices is comparatively uncommon and it is difficult to share the data security of multiple identity authentication technologies. We suggest therefore an identification method for signature-based medical data sharing.

3. Role of IoT in Healthcare System

In the age of e-health systems, the inclusion of IoT has made a significant shift in the paradigms of health care ensuring that data will be freely available and accessible[25]. The prospect of linking 25 billion devices to IOT by 2025 is predicted by industry analysts such as Gartner[26]. This would provide pulse rate measurement medical instruments, blood sugar, heart rates, mood swings and body masses at different stages. Effective IoT networks, later analysed with large data pipelines for practical insights, would be used to produce such data[27]. Currently, thanks to technology such as mHealth and biosensors, the volume of data generated in health systems is increasing exponentially. This involves data derived from separate applications, EHR and Electronic Health Report Results (ePRO). In healthcare systems the function of Big Data is to manage greater data in short periods and thus to reduce calculation time[28]. Big data will forecast illnesses and prevent preventive deaths. Data from different categories of databases, such as insurance and medical reports, must be taken from the collection flow of a data pipeline and then accurate photographs of people can be outlined within a few minutes[29]. Big data in conjunction with IoT health care is very useful because patient data are received as part of IoT and then analysed using big data analytics tools by cloud systems. [30]. Big data pipeline IoT solutions provide frameworks for the management and eventual performance of analytics, medical data collection and stable [31]. Figure 1 illustrates the role of IoT and Big Data in healthcare systems.

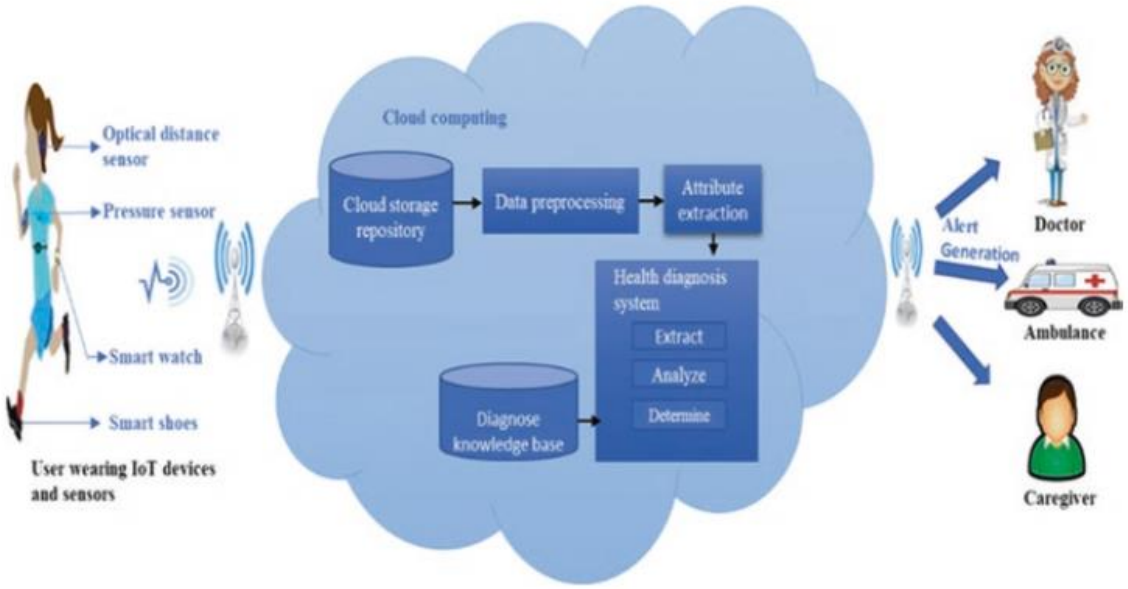

Figure 1: Role of IoT and Big Data in Healthcare System

3.1. Background of Access Control and Authorization Using Role Based Access Control (RBAC)

Data storage security on cloud systems is one of the most difficult issues. Authentication and authorisation are two main processes that provide data storage systems protection. Entry to all data in device after correct confirmation of evidence identities is the method for authentication. Authentication is a means to align username, password or any other authenticity credentials. authentication. Stored data can be available only if authentication factors are used to validate user identification. Authentication is currently performed on two or three levels to provide anyone inside the system with access. Authorization is authorization, on the other hand, to access machine tools until the user has a proof of identity authenticated. Basically, authorization allows the intending person the right to enter the device after adequate authentication. Authorization normally comes after authorization on any device that gives administrator rights for the system. Role Dependent Access Control (RBAC) is a computer systems architecture that provides users with restricted access after the necessary authentication, based upon privileges. This model operates on a system that centres around user functions and permissions. The paper also includes an algorithm for two fish coding, which is explained in the technique section proposed.

3.1.1. Rules for Defining RBAC

The basic rules which are used in RBAC model are shown in Figure 2.

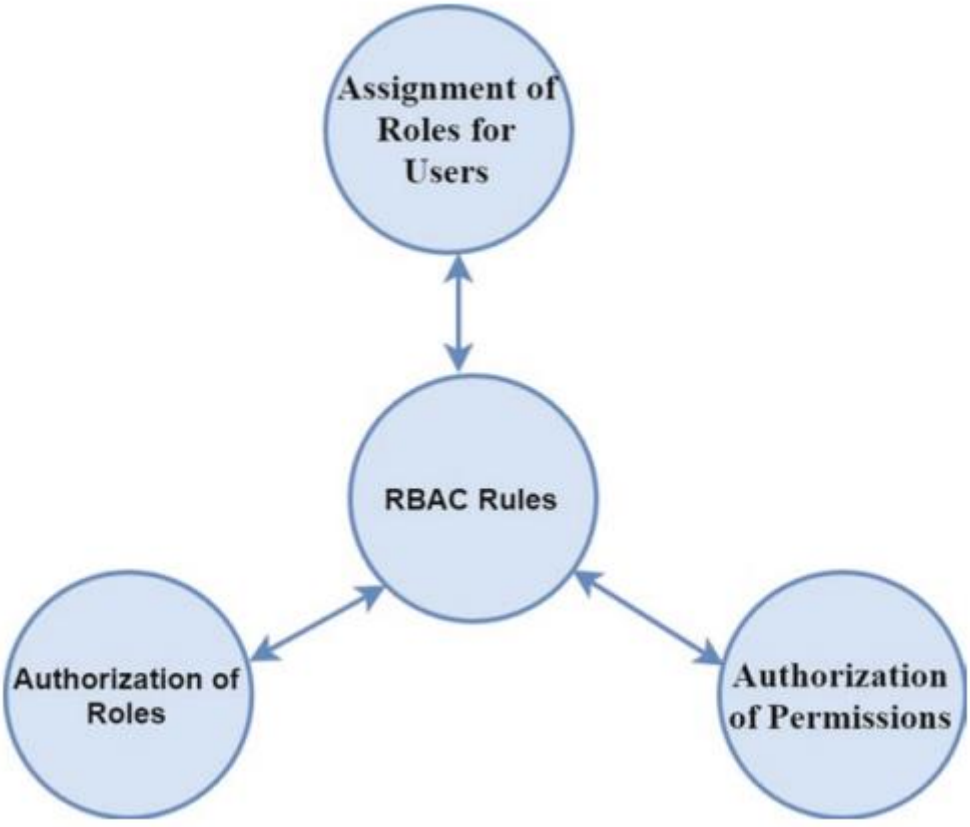

Figure 2: Rules in RBAC model

User assignment: Function is a duty that is delegated to users and users may only perform permissions after assigning tasks.

Role authorization: users are only allowed to play active roles such that users may access only assigned roles that have already been approved.

Permission authority: Users are approved for positions that are active only Authorisation.

4. Proposed Methodology

This section uses two algorithms to protect cloud data, in which the ERBAC model was first and later described as the 2-fish encryption algorithm.

4.1 Extended Role Based Model (ERBAC)

Though RBAC's core reference models prove better in terms of authentication and access control, there are few problems with the ordinary ones. However, there are no requirements for limiting the number of users for the same positions because RBAC reference models allow for many users to play a role. Even when permissions are delegated to functions, users cannot access separate accesses on the basis of criteria under one role. There are also no restrictions on access to data that any user has. In order to take these loopholes into account, all of these conditions need to be fulfilled by the RBAC model. The following measures to meet the constraint in simple reference models are proposed in the Expanded RBAC.

The restriction for users for special functions will be introduced in phase 1. Just certain consumers are added to the position where the data can be used. In phase 2, data storage permissions are placed on users to access confidential data with limitations and reduce the probability for invalid users of data breaking. In step 3, membership status will be introduced in order to access data dependent on position hierarchy for different users under one role.

4.2. Twofish Algorithm

Twofish also has a fiestel structure as symmetrical block cypher. Effective for applications running on smaller processors (intelligent cards) and hardware embedding. It enables users to optimise encryption speed, key configuration and code size for performance equilibrium. Twofish is free of licence, unpatented and free to download. It uses 128, 192 and 256 bits of double-fish encryption. The block size is 128 bits and the encryption algorithm comprises 16 loops. Figure 3 shows the rounding feature of two fish.

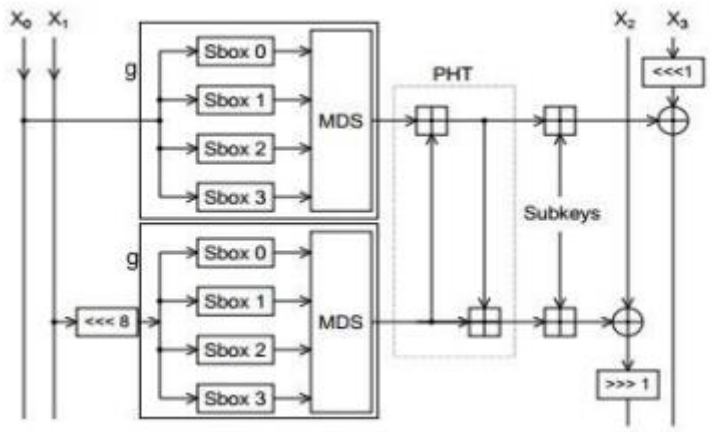

Figure 3: Rounding Function of Twofish algorithm

It encrypts data in this round feature. This round feature encrypts data repeatedly 16 times, then after round 16 the final cypher text [32]. The figure above,

1. On the left, X0 and X1 works by 8 bits of one of the inputs to a g after rotation.

2. The g function contains 4 byte S-boxes, followed by a linear mixing stage (MDS matrix).

3. The findings are paired with a PHT for the two g functions (Pseudo-Hadamard Transform).

4. Two keywords will be added later. That on the right is rotated by 1 bit and the two keywords are XORed to the outcome on the left.

5. Right and left substituted for the next round.

6. The last exchange is reversed after 16 rounds of encryption with four additional xorized keywords creating the actual encrypted text and the cypher text.

Twofish comprises a total of 16 encryption rounds and after 16 encryption rounds we have completed the final 128 bit cypher text[33]. The two-fish encryption algorithm is also good for protection, but the encryption speed is not usable.

The two algorithms (i.e. ERBAC and twofish) are recommended and used for IoT safe storing medical data as seen in Figure 4. This access management model has been developed by the authors to ensure that data is maintained on cloud systems. Model View Controller System (MVC) from Microsoft is used to execute this model. Cloud computing on Microsoft Azure Platform is used to storage IoT medical data. All user information for this programme are contained in the Azure SQL database. Details regarding positions and permissions is also provided in the Azure SQL database. For the storage of medical data on a cloud system, IoT gateway sensors are used and placed in storage account containers. The same data is encrypted to become cypher text and can be saved in Microsoft Azure's database account. The encryption and decryption keys are kept in the local database.

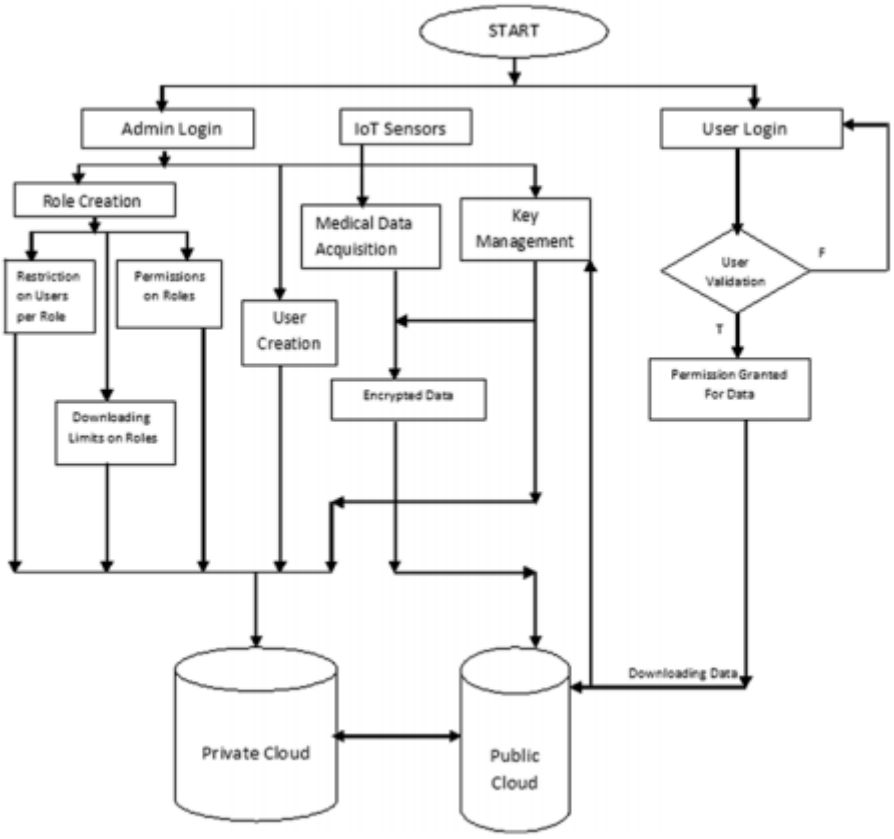

Figure 4: Proposed ERBAC with Twofish for securing storage of medical data on cloud systems

In the photo. 4, the healthcare organization's administrator portal was developed to control and authorise users and roles. Administrators will login to be routed to the main dashboard with passwords. Administrator may build roles on the dashboard and enforce roles authorizations for individual users. The organisation will determine which customer pool is accessible for this model and can limit the usability of patient data information for patients. The dashboard also establishes credentials for various account hierarchies. Model is based on two way user authentication, i.e. the cloud-platform key for the decoding of data records will be emailed to the registered mailbox when successful login happens. In the case of true authentication, 3 attempts to verify passwords are made for a user and the fourth attempt does not allow the user to sign in for the next 24 hours in either hierarchy.

4.3. Proposed Medical Data Clustering

The compilation is an unconventional approach for the exploration of enormous data, and does not support the collection of data objects due to different similarities. Numerous experts have concentrated on the grouping issue, using various methodologies, including taboo looks, genetic calculations, re-enacted strengthening, underground insect conditions, a hybridised method and fake settlements in the honey bee. PSO-GA approximation is proposed for these purposes because it uses the enhancement of PSO calculations internationally to compensate for the absence of a grouping technique.

A novel half PSO-GA calculation is built in this paper for clustering of clinical knowledge by consolidating two PSO and GA enhancement methods. A half-and-half-pSO-

GA stream graph has been shown. In the proposed count, the crossbreed calculation uses dual impact factors to maximise the particles swarm or GA. Ú μ a [0,1] accelerates PSO sway factor. When the PSO sway factor τ looks at 0 there is no effect of PSO on masses at that point. When the impact factor μ is considered 1, PSO acts as normal PSO. The middle individual in the range between 0 and 1 periodically switches factor τ. The moderate value reduced the molecule bounce and improves the look around the competitive arrangement by means of a PSO power. Figure 5 provides the total flow of the clustering mechanism proposed.

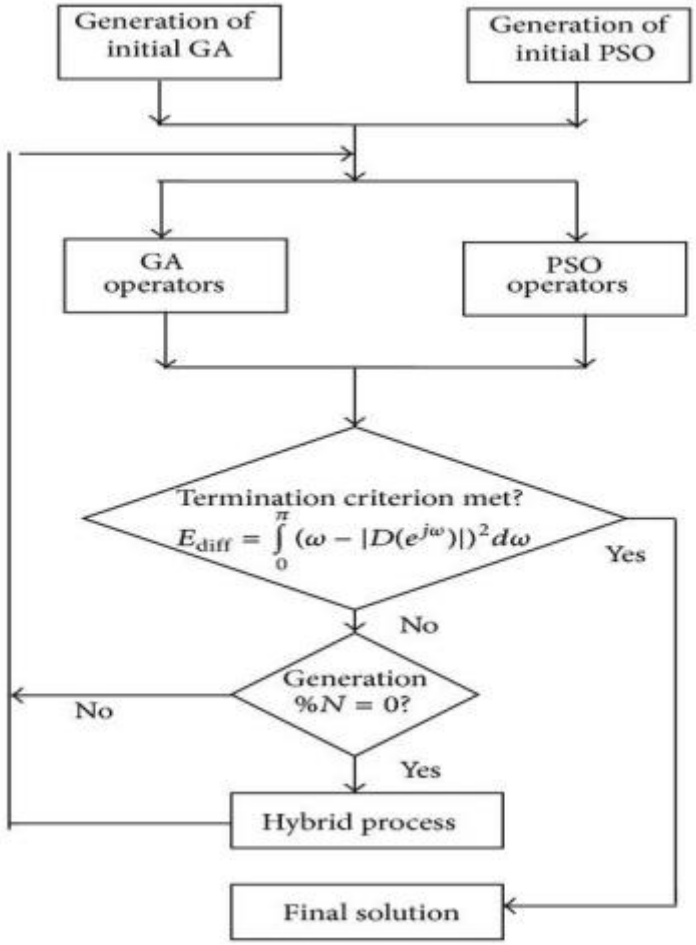

Figure 5: Workflow of PSO-GA algorithm

It depends on the multifactor PSO measure, as it has been successfully shown. Three basic labels are proposed for clustering: focused capabilities, simplification, dynamics. Two opposing goal capacities right away from bat are differentiated by the fact that bunches are reduced and completely separated. We also detail the method of streamlining three sections: molecular representation, pioneer commitment and improved arrangement technique, since improvement is the most critical work to look at large plots. Finally, a chief is used with the most rational Pareto arrangement.

With the administrator option, the GA impact factor μ biszu [0,1] increases. In the event that genetic algorithms μ have an aspect of 0, no human is involved in generating and recombining the genetic algorithm without an effect on humans. The entire populace takes an interesting GA motion if the GA sway factor μ is 1. There are regenerating masses in the mutt

calculation. The resurgence of people in cream figures takes place in 2 stages. PSO is used for masses with PSO sway factor¨ in the 1st level. In a n point, the top(1 – μ) = pop-size persons go directly to persons to come and μ = pop-size persons come from GA managers.

There are many ages in the new cross breed figure. Initialize category n clusters randomly;

$$D_i = \sum_{j=1}^{n} exp\left(-\frac{\|x_i - x_j\|^2}{\left(r_a/_2\right)^2}\right) \quad (1)$$

The exponential rate of the clusters is calculated as given in Eq. (2)

$$* x_p = \frac{1}{n_j}\sum_{n_j - c_i} Z_p \quad (2)$$

The relation between similar records are calculated as given in Eq.(3)

$$p_i(t+1) = \begin{cases} p_i(t) & f(x_i(t+1) \le f(x_i(t))) \\ x_i(t+1) & f(x_i(t+1) > f(x_i(t))) \end{cases} \quad (3)$$

Based on this clustering process will be occurred in the database for retrieving similar medical records. The next section will explains the validation of proposed methodology.

5. Results and Discussion

In this section, the validation of encryption techniques as well as clustering methodology are given in two subsection, which is defined as follows:

5.1. Performance Analysis of Proposed Encryption Methodology

In the below table 1, the performance of proposed ERBAC and twofish algorithm are compared with existing techniques in terms of encryption time for different number of files is presented.

Table 1: The comparison among the proposed techniques in terms of encryption time

Algorithms	**Number of Files**					
	100	**200**	**300**	**400**	**500**	**600**
AES	170	198	201	245	485	512
Blowfish	168	191	187	237	480	501
RBAC	170	180	198	255	459	472
Proposed twofish	152	174	181	201	431	453
Proposed ERBAC	**126**	**146**	**159**	**165**	**216**	**327**

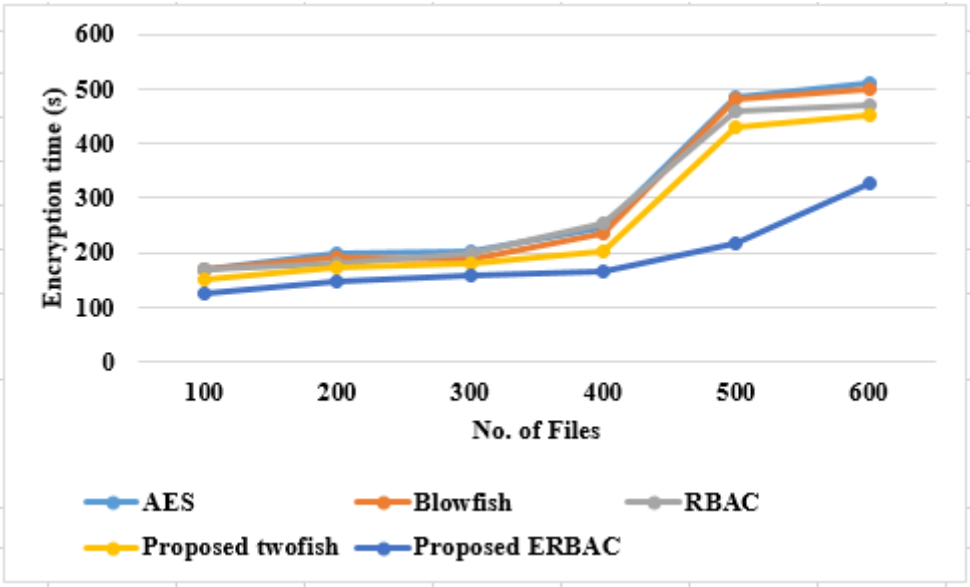

Figure 6: Graphical representation of proposed method in terms of encryption time

The vertical axis in table 1 displays the algorithm's encryption time in seconds. In fact, the encryption time is the start of a test data algorithm before the best possible solution is found. In seconds, we illustrated this time. Under this test the number of files was increased by encoding time, and optimal or near-optimal solutions were found in algorithms later. The suggested algorithm uses two algorithms based on this criteria, and has a better encryption time than Blowfish and AES algorithms. In this diagram, the encryption time of AES was more lengthy, and the Blowfish followed, although the encryption speed of the RBAC algorithm was great. However, the optimal solution achieves a more significant criterion than the time of encryption when the proposed algorithm achieved, in a reasonable time relative to other algorithms, in producing optimal or nearly optimal solutions. The encryption time of the 2fish algorithm, as stated above, is less than ERBAC technology.

5.2. Performance Analysis of Decryption Time

The decryption time is another essential indicator which can be used to measure the performance of the existing algorithms with proposed ERABC and twofish algorithms. The decryption time of the existing algorithms with proposed method is as follows in Table 2:

Table 2: The comparison among the proposed algorithms using the decryption time

Algorithms	**Number of Files**					
	100	**200**	**300**	**400**	**500**	**600**
AES	160	176	195	221	467	497
Blowfish	151	171	172	212	443	487
RBAC	130	167	169	190	430	468
Proposed twofish	142	153	160	184	410	441
Proposed ERBAC	**110**	**135**	**140**	**169**	**390**	**420**

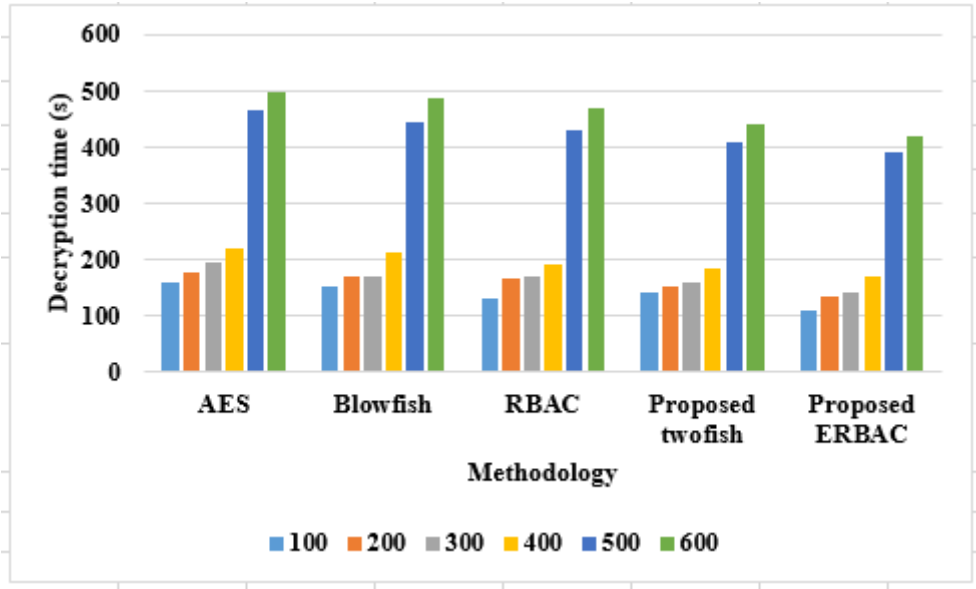

Figure 7: Graphical representation of proposed method in terms of decryption time

Figure 7 illustrates the decryption time of the existing algorithms, and the experimental results show that proposed ERBAC method is the best (leads to the least time), twofish is the second, RBAC is the third, and AES is the worst. The proposed method is better than other three algorithms, and the reason is that it decrypts the more number of files which leads to the shorter time of big files. Therefore, the decryption time of ERBAC is the best. Twofish is better than RBAC and blowfish, and it can be explained that ERBAC inherits this characteristic of some rules from RBAC algorithm. Figure 7 also displays that the decryption time grows with the increase in the number of files.

5.3. Performance Analysis of Proposed Clustering Methodology

In this section, performance of PSO-GA is tested with single algorithms with different medical diseases in terms of clustering accuracy levels. Table 3 explains the validation analysis.

Table 3: Validation analysis of proposed clustering technique

Different Medical Disease Files	Clustering Accuracy (%)			
	GA	PSO	ABC	Proposed PSO+GA
5	69	75	70.23	81
10	69.87	76.41	69.01	86
15	70.15	78.94	69.15	89
20	72.64	80.12	64.23	90.15
25	75.10	81.29	66.74	92.4
30	77.25	83.94	67.19	92.59

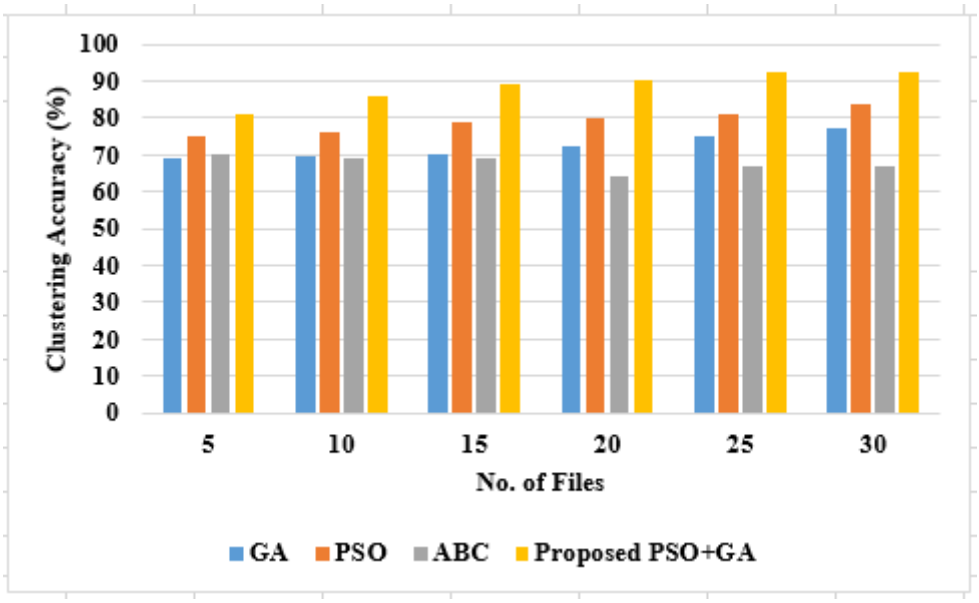

Figure 8: Graphical representation of proposed method in terms of clustering accuracy

From the Table 3, it is clearly stated that the clustering accuracy is higher in the proposed hybrid methodology than single PSO, GA and ABC. When comparing with other techniques, ABC provides less clustering accuracydue to its searching strategy. GA has 70% to 77% of clustering accuracy for different files, where PSO has 76% to 83% of clustering accuracy for those disease files. But, when combining GA and PSO, it achieved 86% to 92% of clustering accuracy by using its efficient sway factors. From the experiments, the proposed hybrid technique achieved better performance.

6. Conclusion

Many malware attacks on now-to-day applications such as e-banking, internet ads, medical data software, etc. Data protection is especially important in cloud computing, and speed is often taken into consideration. The intruders have grew as a result of the increase in data exchanged between networks. In all ways, these people attack the details. To deter certain stuff people are beginning to cover and encrypt their data in various ways. This paper introduces a new expanded role-based access control paradigm and twofish algorithms for multiple healthcare protection functions. This model guarantees protection of cloud-based medical data, with required functions and users constraints. The model introduced an RBAC function that offers the possibility to access the stored records on the basis of a single position with many users. In this model two methods authentications and cryptographic strategies have been employed to securing cloud records. In order to store therapeutic knowledge based on progression of the molecular swarm and the GA, new crossover measurement PSO-GA is also proposed. A global inquiry at the introductory ages is carried out for half PSO GA estimation activities with genetic algorithms and PSO working district survey over ages. In future work to address the encryption speed, the two-fish algorithm is not usable, therefore, an improved two-fish algorithm will be built.

Reference

[1]. Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu, ‘‘Vehicular social networks: Enabling smart mobility,’’ IEEE Commun. Mag., vol. 55, no. 5, pp. 16–55, May 2017.

[2]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, ‘‘Internet of Things: A survey on enabling technologies, protocols, and applications,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.
[3]. W. Wang, S. Yu, T. M. Bekele, X. Kong, and F. Xia, ‘‘Scientific collaboration patterns vary with scholars’ academic ages,’’ Scientometrics, vol. 112, no. 1, pp. 329–343, Jul. 2017.
[4]. X. Wang, Z. Ning, X. Hu, L. Wang, L. Guo, B. Hu, and X. Wu, ‘‘Future communications and energy management in the Internet of Vehicles: Toward intelligent energy-harvesting,’’ IEEE Wireless Commun., vol. 26, no. 6, pp. 87–93, Dec. 2019.
[5]. Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, ‘‘A cooperative quality-aware service access system for social Internet of vehicles,’’ IEEE Internet Things J., vol. 5, no. 4, pp. 2506–2517, Aug. 2018.
[6]. Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, and R. Y. K. Kwok, ‘‘Mobile edge computing enabled 5g health monitoring for Internet of medical things: A decentralized game theoretic approach,’’ IEEE J. Sel. Areas Commun., pp. 1–16, 3rd Quart., 2020.
[7]. R. C. Shit, S. Sharma, D. Puthal, and A. Y. Zomaya, ‘‘Location of things (LoT): A review and taxonomy of sensors localization in IoT infrastructure,’’ IEEE Commun. Surveys Tuts., vol. 20, no. 3, pp. 2028–2061, 3rd Quart., 2018.
[8]. X. Liu, A. Liu, T. Qiu, B. Dai, T. Wang, and L. Yang, ‘‘Restoring connectivity of damaged sensor networks for long-term survival in hostile environments,’’ IEEE Internet Things J., vol. 7, no. 2, pp. 1205–1215, Feb. 2020.
[9]. G. Yang, G. Pang, Z. Pang, Y. Gu, M. Mäntysalo, and H. Yang, ‘‘Non-invasive flexible and stretchable wearable sensors with nano-based enhancement for chronic disease care,’’ IEEE Rev. Biomed. Eng., vol. 12, pp. 34–71, 2019.
[10]. J. Yu, J. Liu, R. Zhang, L. Chen, W. Gong, and S. Zhang, ‘‘Multi-seed group labeling in RFID systems,’’ IEEE Trans. Mobile Comput., early access, Aug. 14, 2019, doi: 10.1109/TMC.2019.2934445.
[11]. Xu, X., Zhu, P., Wen, Q. et al., A secure and efficient authentication and key agreement scheme based on ECC for Telecare medicine information systems. J. Med. Syst. 38(1):9994, 2014.
[12]. Chaudhry, S. A., Naqvi, H., Shon, T. et al., Cryptanalysis and improvement of an improved two factor authentication protocol for Telecare medical information systems. J. Med. Syst. 39(6):1–11, 2015.
[13]. Islam, S. K., and Khan, M. K., Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems. J. Med. Syst. 38(10):135, 2014.
[14]. Zhang, F., Cecchetti, E., Croman, K. et al., Town crier: An authenticated data feed for smart contracts. In: The ACM Conference on Computer and Communications Security. ACM, 2016, 1–13.
[15]. Liu, J., Zhang, Z., Chen, X. et al., Certificateless remote anonymous authentication schemes for WirelessBody area networks. IEEE Transactions on Parallel and Distributed Systems 25(2):332–342, 2013.
[16]. Renuka, K., Kumari, S., and Li, X., Design of a secure three-factor authentication scheme for smart healthcare. J. Med. Syst. 43(5): 133, 2019.
[17]. Al-Bassam, M., SCPKI: A smart contract-based PKI and identity system. In: ACM Workshop on Blockchain, Cryptocurrencies and Contracts. ACM, 2017, 35–40.
[18]. Alexopoulos, N., Daubert, J., Mühlhäuser, M. et al., Beyond the hype: On using Blockchains in Trust Management for Authentication.Trustcom/BigDataSE/ICESS, 2017 IEEE. In: IEEE, 2017, 546–553.
[19]. Pramuditha, P., and Patel, V. M., Face-based multiple user active authentication on mobile devices. IEEE Trans. Inf. Forensics Secur. (TIFS) 14(5):1240–1250, 2019.
[20]. Lin, C., He, D., Huang, X. et al., A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems. IEEE Access 6:28203–28212, 2018.
[21]. S.Hirani. Energy Consumption of Encryption Schemes in Wireless Devices, University of Pittsburgh, 2008.
[22]. P.Ruangchaijatupon, and P.Krishnamurthy. Encryption and power consumption in wireless LANs- N, Telecommunication Program, pp. 148-152, Jan. 2001.

[23]. Anjana Devi, and B. S. Ramya. Two fish Algorithm Implementation for lab to provide data security with predictive analysis, International Research Journal of Engineering and Technology, vol. 4, no. 5, pp.3033-3036, Jan. 2017.

[24]. Much Aziz Muslim, Budi Prasetiyo, and Alamsyah. Implementation Twofish Algorithm For Data Security In A Communication Network Using Library Chilkat Encryption ActiveX, Journal of Theoretical and Applied Information Technology, vol. 84, no. 3, pp.2005-2016, Feb.2016.

[25]. Bhatt, C., Dey, N., &Ashour, A. S. (Eds.). (2017). Internet of Things and big data technologies for next generation healthcare. Cham: Springer.

[26]. Gartner. (2014, March 19). Gartner says the Internet of Things will transform the data center. Retrieved from http://www.gartner.com/newsroom/id/2684616.

[27]. Manogaran, G., Varatharajan, R., Lopez, D., Kumar, P. M., Sundarasekar, R., &Thota, C. (2018). A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generation Computer Systems, 82, 375–387.

[28]. Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A. S., &Satapathy, S. C. (Eds.). (2018). Internet of Things and big data analytics toward next-generation intelligence. Berlin: Springer.

[29]. Dimitrov, D. V. (2016). Medical Internet of Things and Big Data in healthcare. Healthcare Informatics Research, 22(3), 156–163.

[30]. M.Anuradha, T.Jayasankar, PrakashN.B[3], Mohamed Yacin Sikkandar, G.R.Hemalakshmi, C.Bharatiraja,A. Sagai Francis Britto, "IoT enabled Cancer Prediction System to Enhance the Authentication and Security using Cloud Computing," Microprocessor and Microsystems (Elsevier 2020), Vol 78, December, (2020) .https://doi.org/10.1016/j.micpro.2020.103301

[31]. R.ArunPrakash, T.Jayasankar, K.VinothKumar, "Biometric Encoding and Biometric Authentication (BEBA) Protocol for Secure Cloud in M-Commerce Environment", Appl. Math. Inf. Sci., Vol.12, No.1, Jan 2018, pp.255–263.
DOI: http://dx.doi.org/10.18576/amis/12012.

[32]. N. Islam, M. H. Mia, M. F. I. Chowdhury and M. A. Matin, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, (2008).

[33]. L. Singh and R. K. Bharti, "Comparative performance analysis of cryptographic algorithms", International journal of advanced research in computer science and software engineering (IJARCSSE), vol. 3, no. 11, (2013).