Dynamic security and routing strategy-based health care monitoring with IoT in wireless sensor network

[1]Dr. M. Vijayakumar, [2]Dr. Archana Ganesh Said, [3]V.S.Triveni, Professor, [4]Dr.J.Srimathi , [5]Naresh Kumar Sripada, [6]Dr.A.Anandh, [7] Dr.K.P.Malarkodi

[1]Department of Computer Technology, Nandha Arts and Science College, Erode,Tamilnadu, India.
[1]Email ID:Vij370@gmail.com
[2]Assistant Professor, Department of Computer Engineering, AISSMS IOIT, PUNE-01, Pune
[2]Email ID: archana.said@aissmsioit.org
[3]Department of Mathematics, Geethanjali College of Engineering and Technology, Hyderabad
[3]Corresponding Author Email ID: vstriveni@gmail.com
[4]Associate Professor,Department of Information Technology,KPR college of Arts Science and Research
[4]Email Id: sriphd2020@gmail.com
[4]Orchid: http://www.orcid.org/0000-0003-0693-3496
[5]Assistant Professor, Department of Computer, Science and Artificial Intelligence,SR University,Warangal, Telangana, 506371
[5]Email ID: naresh22.in@gmail.com
[6]Associate Professor, CSE, Kamaraj College of Engineering and Technology, SPGC Nagar, K.Vellakulam, Virudhunagar -625701
[6]Email Id:anandhcse@kamarajengg.edu.in
[7]Assistant professor, Department of computer application, Sri Krishna Arts and science college, Coimbatore
[7]Email ID: malarkodikp@skasc.ac.in

KEYWORDS

Data security; Secure routing; Healthcare monitoring; Mentally disabled; RSDSM

Abstract

Wireless sensor networks are frequently utilized because they enable the provision of at least a range of access services. It is currently being used in the healthcare industry to monitor the patients. To do analysis and make decisions, the data gained through monitoring has been gathered in various cloud environment servers and places. This scenario faces various challenges in recent Internet of Things devices in data security and route security. Such threats affect security performance and decision-making. Although several data encryption and routing techniques have been explored in the literature, they often fall short of achieving the desired level of security. An effective service-centric data security and routing solution is proposed to address this problem. The method focused on monitoring the mentally disabled on the working of their anatomy and updating the data to the cloud data server. The technique utilizing both IoT devices and the infrastructure of a wireless sensor network, which includes sensor nodes. This technique keeps track of various physiological parameters, including heart rate, temperature, and blood pressure. The features monitored have been transmitted to the cloud data server which is updated in the database. The data transmission is performed by

choosing an optimal route by measuring route-specific data security measure value for different routes, which is measured based on the number of IoT devices, Hop count, transmission history of the route, and each IoT device. Similarly, the data security is enforced by adapting Feature Orient Adaptive Encryption scheme which considers the source which generates the data and request.

1. Introduction

The information and communication technology growth at each second and the recent development of communication technology has been used in several problems. The medical society and health care environment adapt various technologies, e.g., data mining for cardiovascular disease diagnosis (Moses &Chelliah, 2015). The wireless sensor network is the one that is being used to perform data collection in various environments. It comes with a set of sensors and involves in cooperative transmission. In the same sense, it has been used in monitoring the health care conditions of the mentally disabled. The mentally challenged people are not capable of conveying the exact illness which challenges the medical practitioner in treating the person by providing exact treatment. This increases the requirement of decision-making systems that should monitor the health conditions of the patients and according to that it should generate recommendations, or it should update to a database with the data monitored.

The data being monitored by any monitoring system becomes huge size. Due to their increased cost, the firms are unable to maintain data servers with greater spacing. This motivates the organizations to move towards a cloud environment that supports the organizations in maintaining the data with the least cost. The cloud environment provides various services in different levels and layers. The wireless sensor network is used to transfer and update the data servers with the information created from monitoring people with mental disabilities. The data present in the cloud can be accessed through several services by decision-making systems as well as medical practitioners.

The service accessed by the medical practitioner and the monitoring devices transmits the data through the routes available in WSN which consists of IoT devices as part of that (Vijayakumar, 2023). The presence of such IoT devices is not trustable and they would leak data and perform different threats to the system. Additionally, a variety of individuals have access to the data stored in the cloud, and they may utilize it for numerous illicit and harmful purposes. So, that securing the data at both data and route level becomes a challenging task.

The route level attack is performed by the set of IoT devices, and the mitigation of the threat has been performed in several ways. When a malicious node is present in the path, it can engage in illegal activities by dropping packets to carry out eavesdropping attacks, altering data values to carry out modification attacks, or choosing a longer route to increase latency numbers while carrying out additional attacks. To mitigate such threats there are several approaches available that perform the detection based on different features. Still, they suffer to achieve higher performance in both security and other factors. This can be avoided by performing routing by considering different factors to improve the security performance. According to this, a dynamic service-centric secure routing scheme is presented in the article.

On the other side, data security has been enforced by monitoring systems. To put it simply, various encryption techniques are used to protect data that is only accessible by specialized persons or equipment. The use of public, AES, DES approaches of data encryption does not help to challenge the adversaries as they can read the data encrypted by different users. To challenge this, there are several approaches available that would use profile data in the selection of scheme and key. Still, they suffer to achieve the performance, and by considering this, a novel service-specific dynamic security scheme has been presented in this paper.

2. Interconnected Work

Different approaches are presented earlier near data security and secure routing towards WSN with IoT devices. This section details the set of approaches around cloud and WSN with IoT devices. (Hajji &Leghris & Douzi, 2018) discusses a multi-constraint adaptive routing (MCAR) system that employs the topology tree for scheduling with node energy. Similar to this, an energy-based partitioning approach for route selection is provided in (Hasan & Al-Rizzo & Gunay, 2017). In (Gangwar & Tyagi & Soni (2018), an adaptive scheduling technique is introduced that schedules the nodes with higher lifetime based on location, activity, and traffic conditions. Similar to this, in (Elma & Meenakshi), 2018, the energy of the nodes determines how they are clustered and how the cluster head is chosen. In order to minimize retransmission, Tan et al. (2018) perform scheduling by adopting a greater duty cycle and energy of nodes.

By modifying the Kalman filter, (Aziz et al., 2019) addresses the coverage issue and extends the network lifetime. Similar to this, (Lazrag & Saadane & Aboutajdine, 2018) presents secure routing using a game-theoretic approach that can decrease power, balance, and traffic with the adaptation of ECC. The trust-orient secure routing strategy is introduced in (Saini & Ahlawat, 2019). It incorporates a number of features, such as energy conservation, trust-based least-hop route identification, and key exchange-based authentication. Similar to this, a trust-based approach that takes into account nodes' continued right behavior throughout route selection is provided in (Navami & Basarkod, 2017). In order to reduce energy usage, the best energy-based secure routing system is described in Kavitha and Geetha (2019). To protect the data saved in WSN, (Ren et al., 2018) implemented blockchain technology to enforce security. Digital currency is given to the data saved in the WSN nodes; the amount of the reward varies according to the amount of data stored. To handle storage and access control, two distinct blockchains are created and kept up to date. Due to its implementation of Proof of Work (PoW), the approach replaces Provable Data Possession (PDS). The author of (Ramezan & Leung & Chen, 2018) addresses the issue of routing in WSNs that are enforced using blockchain technology. The author introduces a blockchain-based contractual routing system called (BCR), which is designed to manage IoT devices in the network and enable effective, secure routing. A centralized authority oversees the management of various sensors' identities and grants permission for communication across various devices in this technique.

The author of (Yang et al., 2019) provides a thorough analysis and addresses the several difficulties associated with combining blockchain algorithms for WSN with IoT devices. In order to increase security, Yang et al. (2019) describe how routing in WSNs employing blockchain technology is carried out using reinforcement learning techniques. Adversaries cannot tamper with

the routing data traced by the approach. The source (Reyna et al., 2018) offers contradiction-based encryption solutions for data security that encrypt data packets without using redundancy using signatures or checksums.The signcryption technique is described in (Iqbal et al., 2019) to enable secure communication in biosensor nodes. It can be used in both offline and online modes. In offline mode, the majority of the work is done without any knowledge of the patient data, and in online mode, the patient data is used for very few operations. Different challenges call for different techniques, and policy-based approaches have been employed in access limitation, where users are unable to access certain data (Waheed & Hanamgond, 2015). Under other conditions, an additional analysis is carried out. Several taxonomies that have been used to restrict access to the data can be applied to it (El-Booz &Attiya & El-Fishawy, 2015). The taxonomy is employed to secure health care data and is evaluated for effectiveness (Chidambaram et al., 2016). When providing data security, the sensitivity of the data should be taken into account. In order to address this, a hierarchical sensitive support (HSS) based access control strategy is presented (Antonidoss, 2019). This approach maintains distinct taxonomies against access control and applies access limitation based on the value found in the taxonomy. Similar to this, access control has made use of the data's context. According to Byun and Kwak (2014), the approach modifies the scenario recognition strategy for access control. In (Lo & Yang & Guo, 2015), a hybrid approach to role- and attribute-based access control is described. This approach uses attribute-level access control to provide data security while restricting users based on their roles. Every technique makes sacrifices in order to attain improved routing and data encryption performance.

3. Service Centric Data Security and Routing Scheme (SCDSRS)

The proposed service-centric data security and routing scheme monitors the health features of the mentally challenged and transmits the data to the cloud data server by accessing a service. The data transmission is performed by selecting a route according to route-specific data security measures (RSDSM). Similarly, the method enforces data security by encrypting the data by using Feature orient adaptive encryption (FOAE) scheme. The approach refreshes the medical practitioners' interface in addition to updating the data on the cloud. In order to handle mentally challenged patients, the medical professional uses the decisive support system to carry out various procedures. This section covers the thorough approach. Fig. 1 depicts the architecture of the suggested service-centric data security and routing scheme-based healthcare monitoring system. It displays the several functional components of the suggested model, each of which is covered in detail in this section.

3.1 Healthcare Monitoring

The mentally disabled are monitored for their anatomic and details of blood pressure, heart rate, temperature, and other conditions. Such data are monitored with the support of different biological sensors attached to the body of the mentally challenged. Such details sensed are updated to the cloud server. Through the assistance of sensor nodes that are situated far from the patients' actual locations, the cloud servers are accessible. In order to get to them, the algorithm determines a set of routes and gathers information such as the quantity of available sensor nodes and IoT

devices. In order to choose the best route, the approach also carries out route discovery and route selection based on the characteristics of the route and the historical data of various transmission routes. Data encryption using the FOAE scheme has been applied, and data transfer has taken place over a chosen path. Both the medical professional's interface and the cloud server have received updates from the transmitted data.

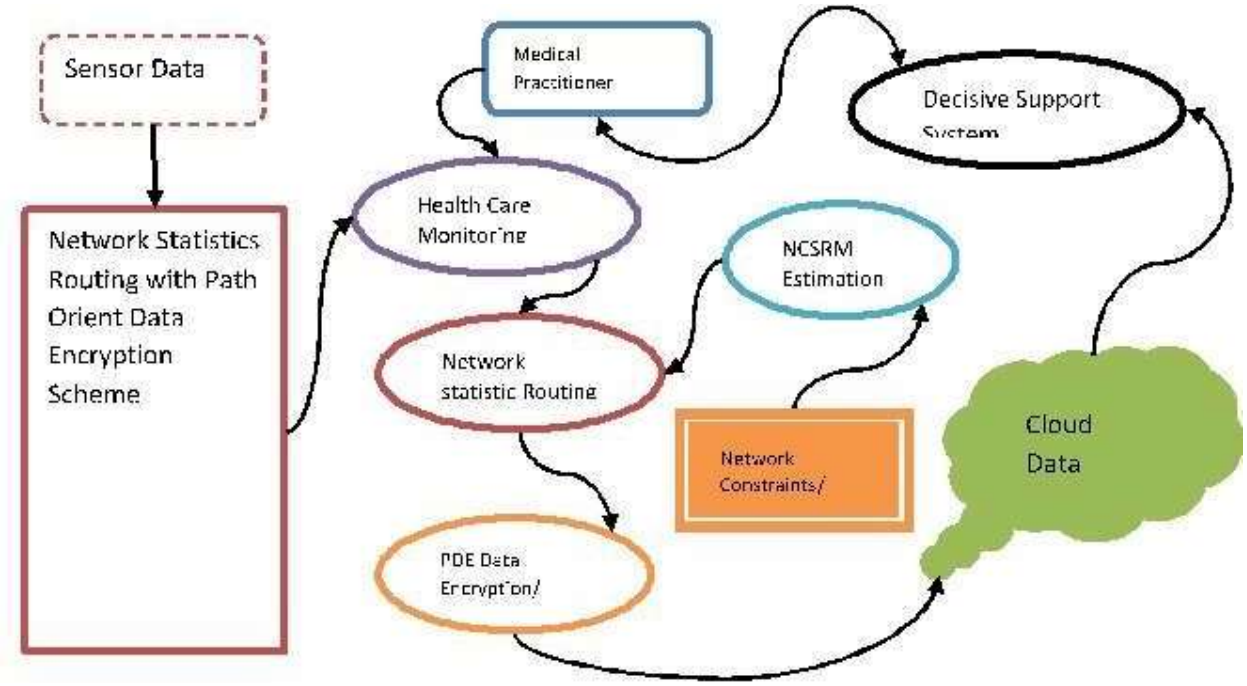

Fig. 1. The suggested statistics-based routing architecture uses path-oriented data encryption.

3.2 RSDSM Routing

There are multiple ways for the wireless sensor network to get to the cloud servers. The process starts by determining the range of paths that go to them. The method counts the number of sensors and IoT devices that are currently in use for each route before determining how many hops the route has. Additionally, the transmission history for every route and IoT device has been gathered from the localized data table. The approach uses the information gathered to calculate the Structural Routing Security (SRS) value based on the number of IoT devices and other sensor nodes along the path. In a similar vein, the transmission history is used to gauge Behavioral Routing Security (BRS). Additionally, the technique uses the transmission history of IoT devices to calculate the value of Device Centric Route Security (DCRS). The technique calculates the RSDSM value using each of these metrics, and then uses that value to determine which route should be used to transmit data.

3.3 RSDSM Routing Algorithm

The above-discussed Algorithm 1 (Fig. 2) explains how the structural, behavioural, and device-centric route security measures are estimated. The approach calculates the value of RSDSM based on the SRS, BRS, and DCRS values. The approach chooses the best and safest path for data transmission based on the value of RSDSM.

Algorithm 1 RSDSM Routing Algorithm

Require: Transmission History TH, Sensed Data SD
Ensure: Route R
Read TH and SD
Identify list of route
$Rol \leftarrow \sum_{i=1}^{size(TH)} (TH(i).Route \ni Rol) \cup (\sum Routes \in Rol)$
for all Route R **do**
Identify number of IoT devices
$NIoT \leftarrow \sum IoT \in R$
Collect the traces of Route R as RT
$RT \leftarrow \sum_{i=1}^{size(TH)} TH(i).Route == R$
Compute structural route security
$SRS \leftarrow \frac{NIoT}{size(R)}$
Compute behavioral route security
$BRS \leftarrow \frac{\sum_{i=1}^{size(RT)} RT(i).state==R}{size(RT)}$
$DCRS \leftarrow \frac{\sum_{i=1}^{NIOT} \sum_{j=1}^{size(RT)} RT(j).Route(NIOT(i)).Tag==Transmit}{size(RT)}$
$RSDSM \leftarrow \frac{BRS}{SRS} \times DCRS$
end for
Route $R \leftarrow MAX(RSDSM)$

Fig. 2. RSDSM Routing Algorithm

3.4 FOAE Data Encryption

The Feature Orient Adaptive Encryption algorithm is used in this method to enforce data security. The procedure locates the data and counts the attached details in order to accomplish this.The biological data would have various information. Not all of them will be transmitted at each transmission. For example, the temperature and heart rate will be transmitted in a little delay whereas the rest of the details are transmitted and updated more frequently. According to this, the method analyzes the data to be transmitted and finds the number of sensitive and non-sensitive items. According to that, the method selects the data encryption scheme, if the sensitive items are higher in the data, then it would select the most secure approach like ECC otherwise, it would select a nominal approach to perform data encryption. Similarly, the approach does re-encryption to accomplish data transfer based on the number of IoT in the path.

3.5 FOAE Data Encryption Algorithm

The data is read by the feature-oriented adaptive encryption system, which then determines which parts of the data are sensitive and which are not. In order to choose the scheme and key, it

also counts the number of IoT devices along the path. According to that the data has been encrypted for two times as re-encryption to improve the data security (see Algorithm 2 on Fig. 3).

Algorithm 2 FOAE Data Encryption Algorithm

Require: Data D, Schemeset SS, Keyset Ks, Route R
Ensure: Encrypted Data ED
Read D, SS, Ks
Identify number of sensitive items
$NSI \leftarrow \sum_{i=1}^{size(D)} D(i).Type = Sensitive$
Identify number of non sensitive items
$NNSI \leftarrow \sum_{i=1}^{size(D)} D(i).Type = NonSensitive$
if $NSI > NNSI$ **then**
Scheme $s \leftarrow \int_{size(SS)}^{i=1} SS(i).Standard == Max$
else
Scheme $s \leftarrow \int_{size(SS)}^{i=1} SS(i).Standard == Moderate$
end if
Encrypted data $Ed = PerformDataEncryption(D, s, Random(Ks))$
Compute number of IoT devices $NIoT = \sum IoTDevices \in R$
if $NIoT > (Size(R) - NIoT)$ **then**
Scheme $s \leftarrow \int_{size(SS)}^{i=1} SS(i).Standard == Max$
else
Scheme $s \leftarrow \int_{size(SS)}^{i=1} SS(i).Standard == Moderate$
end if
Encrypted data $Ed = PerformDataEncryption(D, s, Random(Ks))$

Fig. 3. FOAE Data Encryption Algorithm

Algorithm 3 Treatment Recommendation Algorithm

Require: Biological Trace BT, Data D
Ensure: Treatment Recommendation TR
Read BT, D
for all disease Dis **do**
Compute multi Bio Feature disease support (MBFDS)
$MBFDS \leftarrow \frac{\sum_{i=1}^{size(BT)} \sum_{j=1}^{size(D)} BT(i) \in D(j) \wedge D(j).value > Th}{size(BT)}$
end for
Disease $Dis \leftarrow$ disease with maximum $MBFDS$ value
Recommendation:
$TR \leftarrow \sum_{i=1}^{BT} BT(i).Disease = DIS \wedge BT(i).Treatment == Success$

Fig. 4. RSDSM Routing Algorithm

3.6 Decision Support System

The proposed decisive support system obtains updated through live biological sensors and with the support of a wireless sensor network. Such data received has been used in making automated decisions to support the medical practitioner. The system automatically populates the

biological factors in the interface as well as with the data obtained, the method runs a decision analysis with the features obtained. The method computes Multi Bio Feature Disease Support (MBFDS) for various diseases. The risk factor for various diseases is measured according to the MBFDS value. According to that, the decisive support system list and rank the possible risk factors using which the medical practitioner would make decisions and generate treatment recommendations to the on floor medical team.

The system of decisive support analyzed the provided data and traces. The method calculates the multi bio feature disease support value for each detected disease using these. The approach determines which one is the riskiest by using the value of MBFDS. The approach produces recommendations to the physician for the detected ailment. For further information, see Fig. 4's Algorithm 3.

4. Results and Discussion

The suggested service-oriented security and routing approach have been put into practice and their effectiveness has been assessed across a range of criteria. The protocol has been hardcoded, and the method's performance has been verified by adjusting the network's various characteristics. The obtained findings are contrasted with several accessible methods.

Parameter	Value
Number of sensor nodes	170210
Number of IoT devices	3040
Cloud Environment	Microsoft Azure
Programming	Advanced Java

Table 1. Environment Details

Table 1 presents the specifics of the simulation environment that was taken into account for assessing the suggested approach's performance. The number of sensor nodes and Internet of Things (IoT) devices in the environment is changed to conduct the study. Every test case's outcome has been documented and contrasted with the outcomes of alternative techniques.

	50 nodes	100 nodes	200 nodes
MCAR	74	77	83
BCR	78	82	86
Trust Orient	82	86	89
RSDSM	87	92	96

Table 2. Performance analysis on security performance

The evaluation results on security performance introduced by various methods are shown in Table 2. By altering the quantity of sensor nodes in the network, the approaches' effectiveness is assessed. The suggested RSDSM algorithm has outperformed alternative techniques in every instance.

Figure 5 shows how well various approaches perform in the development of security. In every instance, the suggested RSDSM algorithm outperformed alternative techniques in terms of performance.

The evaluation results on routing performance introduced by various approaches are shown in Table 3. By altering the quantity of sensor nodes in the network, the approaches' effectiveness is assessed. The suggested RSDSM algorithm has outperformed alternative techniques in every instance.

The number of nodes in the network varies to determine the routing performance generated by various strategies. Figure 3 displays the obtained results. Compared to alternative approaches, the suggested RSDSM produced better routing performance.

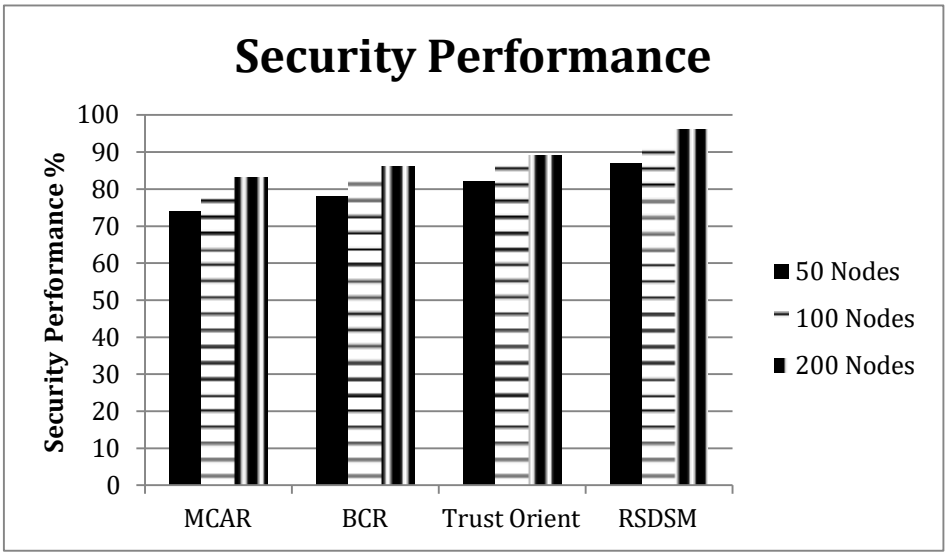

Fig. 5. Analysis on security performance

	50 nodes	**100 nodes**	**200 nodes**
MCAR	75	78	82
Trust Orient	81	83	86
RSDSM	84	89	94
NSRPDE	87	93	98

Table 3. Performance analysis on Routing Performance

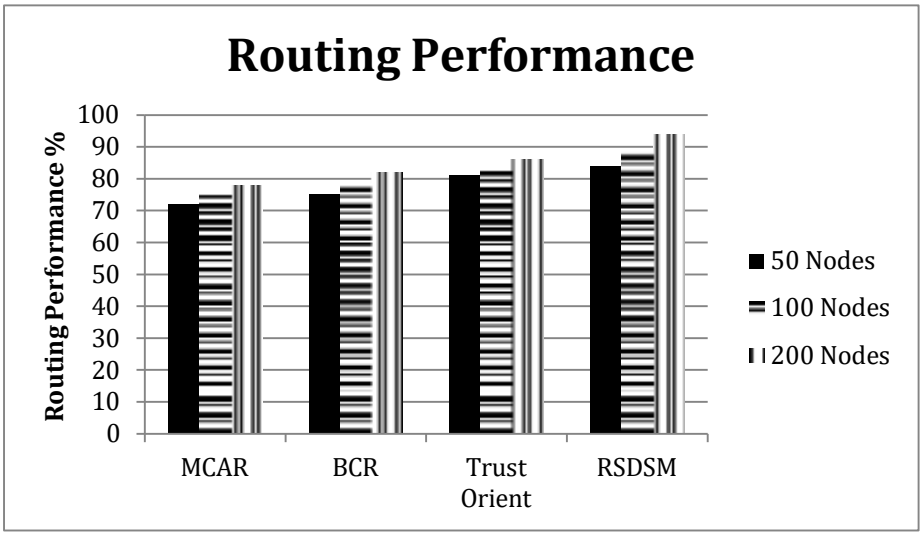

Fig. 6. Analysis on routing performance

	50 nodes	100 nodes	200 nodes
Policy Based	67	71	75
HSS	71	76	79
Signcryption	76	78	82
RSDSM	84	89	93

Table 4. Analysis on encryption/decryption performance.

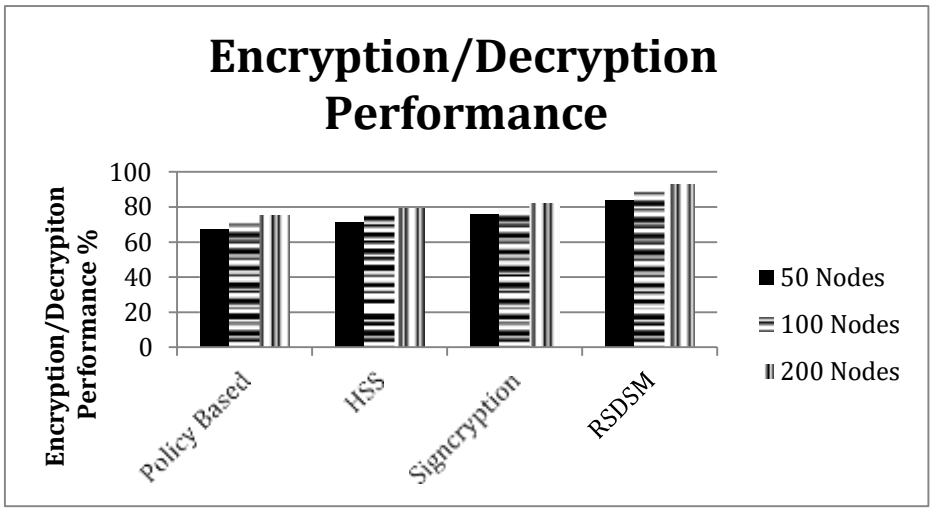

Fig. 7. Analysis on encryption / decryption performance

The evaluation results on data encryption and decryption performance introduced by various approaches are shown in Table 4. By altering the quantity of sensor nodes in the network, the

approaches' effectiveness is assessed. The suggested RSDSM algorithm has outperformed alternative techniques in every instance.

The number of nodes in the network varies to determine how well different approaches perform in encryption and decryption. The suggested RSDSM methodology has outperformed alternative methods in every test case.

	50 nodes	100 nodes	200 nodes
Policy Based	73	79	87
HSS	71	76	79
Signcryption	67	71	76
RSDSM	54	59	63

Table 5. Performance analysis on Time Complexity.

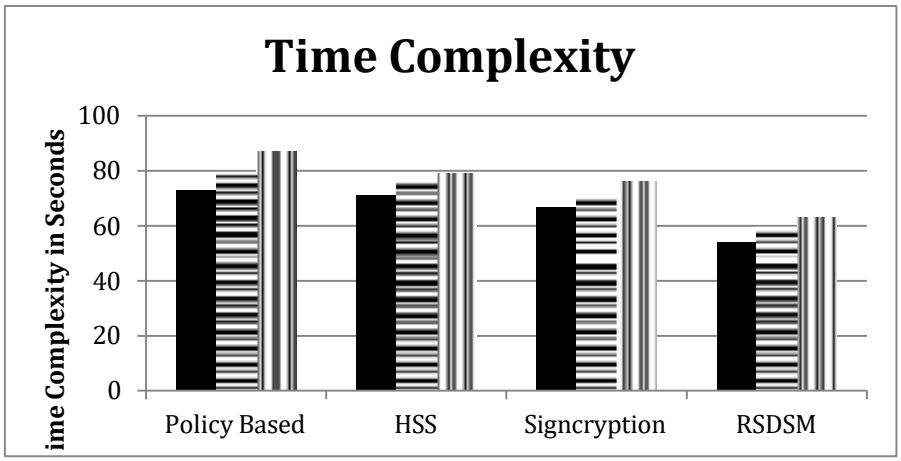

Fig. 8. Time Complexity

In Figure 8, the temporal complexity of several algorithms is quantified and compared. In comparison to other approaches, the suggested RSDSM algorithm has achieved less time complexity.

5. Conclusions

This research study introduced a new service-oriented dynamic security and routing approach to improve WSN healthcare monitoring performance. The method transfers the data to the cloud server while keeping an eye on the patients' health. The approach finds the path and identifies the list of IoT devices on each one in order to accomplish data transmission. It computes the RSDSM value based on the transmission history of various IoT and sensor nodes. The technique chooses the best transmission path based on the value of RSDSM. To protect the data against alteration attempts, the technique also modifies FOAE encryption. Compared to alternative methods, the technology enhances routing and encryption-decryption performance.

References

Antonidoss, A. (2019). Real-Time Hierarchical Sensitivity Measure-Based Access Restriction for Efficient Data Retrieval in Cloud. In: Satapathy, S., Bhateja, V., Somanah, R., Yang, XS., Senkerik, R. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, vol 862. Springer, Singapore. https://doi.org/10.1007/978-981-13-3329-3_18

Aziz, N.A.A., Ibrahim, Z., Aziz, N.H.A., Aziz, K.A. (2019) Simulated Kalman filter optimization algorithm for maximization of wireless sensor networks coverage. In: 2019 International Conference on Computer and Information Sciences (ICCIS):1–6. 10.1109/ICNSC.2009.4919346

Byun YS, Kwak J. Context aware based access control model in cloud data center environment. In: Frontier and Innovation in Future Computing and Communications (FIFCC), Vol. 301. Springer; 2014: 515-524.

Nithya Chidambaram, Pethuru Raj, K. Thenmozhi, Rengarajan Amirtharajan, "Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique", International Journal of Digital Multimedia Broadcasting, vol. 2016, Article ID 8789397, 6 pages, 2016. https://doi.org/10.1155/2016/8789397

S. A. El-Booz, G. Attiya and N. El-Fishawy, "A secure cloud storage system combining Time-based One Time Password and Automatic Blocker Protocol," *2015 11th International Computer Engineering Conference (ICENCO)*, Cairo, Egypt, 2015, pp. 188-194, doi: 10.1109/ICENCO.2015.7416346.

El Hajji, Fouad & Cherkaoui, Leghris & Khadija, Douzi. (2018). Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks. Journal of Communications and Information Networks. 3. 67-83. 10.1007/s41650-018-0008-3.

Elma, K.J., Meenakshi, S.(2018) Network lifetime maximization in wireless sensor network with multiple sink nodes. International Journal of Applied Engineering Research 13:337–34.

Gangwar, D., Tyagi, S., Soni, S. (**2018)**Network lifetime maximization in wireless sensor network with multiple sink nodes. Discovery 54(**7**):284–290.

Hasan, M., Al-Rizzo, H., Gunay, M. (2017) Lifetime maximization by partitioning approach in wireless sensor networks. EURASIP Journal on Wireless Communications and Networking 2017: 39.

Iqbal, J., Umar, A.I., Amin, N.,Waheed, A. (2019) Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain. International Journal of Distributed Sensor Networks 15(**9**).

Kavitha, M., Geetha, B.G.(2019) An efficient city energy management system with securerouting communication using WSN. Cluster Computing 22(**6**):13131–13142, https://doi.org/10.1007/s10586-017-1277-6

Lazrag, H., Saadane, R., Aboutajdine, D.(2018) A game theoretic approach for optimal and secure routing in WSN. In: Abraham, A., Haqiq, A., Ella Hassanien, A., Snasel, V., Alimi, A.M. (eds.)Proceedings of the Third International Afro-European Conference for Industrial Advancement – AECIA:218-228. Springer International Publishing, Cham.

Lo, N.W., Yang, T.C., Guo, M.H. (2015) An attribute-role based access control mechanism for multitenancy cloud environment. Wireless Personal Communications 84(**3**):2119–2134.

Moses, D., Chelliah, C. D. (2015) A survey of data mining algorithms used in cardiovascular disease diagnosis from multi-lead ECG data. Kuwait J. Sci. 42 (**2**):206-235.

Navami Patil, G.M., Basarkod, P.I.(2017) Trust model for secure routing and localizing malicious attackers in WSN. In: Vishwakarma, H.., Akashe, S. (eds.) Computing and Network Sustainability:1–9. Springer Singapore, Singapore.

Ramezan, G., Leung, C., Chen, J. (2018) Ablockchain-based contractual routing protocol for the internet of things using smart contracts. Wirel. Commun. Mob. Comput.,https://doi.org/10.1155/2018/4029591

Ren, Y., Liu, Y., Ji, S., Sangaiah, A.K., Wang, J. (2018) Incentive mechanism of data storage basedon blockchain for wireless sensor networks. Mobile Information Systems.

Reyna, A., Martın, C., Chen, J., Soler, E., Dıaz, M. (2018) Onblockchain and its integration withIoT challenges and opportunities. Future Generation Computer Systems 88:173–190, https://www.sciencedirect.com/science/article/pii/S0167739X17329205

Saini, K., Ahlawat, P. (2019) A trust-based secure hybrid framework for routing in WSN. In: Sa, P.K., Bakshi, S., Hatzilygeroudis, I.K., Sahoo,M.N. (eds.) Recent Findings in Intelligent ComputingTechniques:585–591. Springer Singapore, Singapore.

Tan, J., Liu, A., Zhao, M., Shen, H., Ma, M. (2018) Cross-layer design for reducing delay and maximizing lifetime in industrial wireless sensor networks. EURASIP Journal on Wireless Communications and Networking 2018(**1**).

Waheed, M.A., Hanamgond, A. (2015) Cloud security using sap-shared authentication protocol. International Journal of Computer Science and Mobile Computing 4:106–113.

Yang, J., He, S., Xu, Y., Chen, L., Ren, J. (2019) A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. Sensors (Basel, Switzerland) 19(**4**): 970.

M. Vijayakumar. (2023) Network statistics-based routing and path orient data encryption scheme for efficient healthcare monitoring with IoT in WSN. International Journal of Communication Systems, 48(6): 1-12. https://doi.org/10.1002/dac.5361.