IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 9, September 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109018 |

Survey of Network Intrusion Detection Methods from the Perspective of the Knowledge Discovery in Data Base Process

Ms.V.Thilagavathi[1], Dr. V. Vijayadeepa[2], M.Sc.,MCA.,M.Phil.,Ph.D.,

Research Scholar, Department of Computer Science, Muthayammal College of Arts and Science

Rasipuram, Tamilnadu, India

Head/ Department of Computer Application, Muthayammal College of Arts and Science

Rasipuram, Tamilnadu, India

ABSTRACT: The identification of community attacks on information and communication structures has been a focal point of the research community for years. Network intrusion detection is a complicated task which affords a large number of challenges. Many attacks presently go undetected, whilst more modern ones emerge due to the proliferation of linked devices and the evolution of verbal exchange generation. In this survey, we overview the strategies that have been implemented to gather community information with the motive of developing an intrusion detector, but contrary to previous evaluations in the area, we analyses them from the viewpoint of the Knowledge Discovery in Databases (KDD) method. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation. We mainly focus on data reliability protection; give an identity-based cumulative signature design with a designated verifier for wireless sensor networks. According to the advantage of cumulative signatures, our design not only can remain data reliability, but also can condense bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based cumulative signature idea is strictly presented based on the computational Diffie-Hellman statement in random oracle form.

KEYWORDS: Big data, wireless sensor network, identity based, data aggregation, enforceability, aggregate signature, coalition attack, designated verified

I. INTRODUCTION

As Location-Enabled mobile devices proliferate, location- based services are rapidly becoming immensely popular. Most of the current location-based services for mobile devices are based on users' current location. Users discover their locations and share them with a server. In turn, the server performs computation based on the location information and returns data/services to the users. In addition to users' current locations, there is an increased trend and incentive to prove/validate mobile users' past geographical locations. This opens a wide variety of new location-proof based mobile applications. Described several such potential applications store wants to offer discounts to frequent customers. Customers must be able to show evidence of their repeated visits in the past to the store. A company which promotes green commuting and wellness may reward their employees who walk or bike to work. The company may encourage daily walking goals of some fixed number of miles. Employees need to prove their past commuting paths to the company along with time history. This helps the company in reducing the healthcare insurance rates and move towards sustainable lifestyle. On the battlefield, when a scout group is sent out to execute a mission, the commanding center may want every soldier to keep a copy of their location traces for investigation purpose after the mission. In big data era, digital universe grows in stunning speed which is produced by emerging new services, such as social network, cloud computing and internet of things. Big data are gathered by omnipresent wireless sensor networks, aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras, etc. And the wireless sensor network is one of the highly anticipated key contributors of the big data in the future networks. Wireless sensor

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109018 |

networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has very broad application prospects both in military and civilian usage, including military target tracking and surveillance, animal habitats monitoring, biomedical health monitoring, critical facilities tracking. It can be used in some hazard environments, such as in nuclear power plants.

II. RELATED WORK

The concept of image inpainting was first introduced by Herve Debar , Marc Dacier , Andreas Wespi,[1] Intrusion-detection systems aim at detecting attacks against computer systems and networks, or against information systems in general, as it is difficult to provide provably secure information systems and maintain them in such a secure state for their entire lifetime and for every utilization. In this paper, we introduce a taxonomy of intrusion-detection systems that highlights the various aspects of this area. This taxonomy defines families of intrusion-detection systems according to their properties. Tingshan Huang, Harish Sethu and Nagarajan Kandasamy [2] Based on theoretical insights proved in this paper, we propose a new distance-based approach to dimensionality reduction motivated by the fact that the real-time structural differences between the covariance matrices of the observed and the normal traffic is more relevant to anomaly detection than the structure of the training data alone. P. Garcıa-Teodoroa, J. Dı´az-Verdejoa, G. Macia-Fernandeza, E. Va zquezb [3]This paper begins with a review of the most well-known anomaly-based intrusion detection techniques. Then, available platforms, systems under development and research projects in the area are presented. Finally, we outline the main challenges to be dealt with for the wide scale deployment of anomaly-based intrusion detectors, with special emphasis on assessment issues. Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller [4] Intrusion detection is an important area of research. Traditionally, the approach taken to find attacks is to inspect the contents of every packet. The paper provides a classification of attacks and defense techniques and shows how flow-based techniques can be used to detect scans, worms, Botnets and Denial of Service (DoS) attacks. Borja Molina Coronado, Usue Mori, Alexander Mendiburu and Jose Miguel-Alonso [5]As such, we discuss the techniques used for the collecion, preprocessing and transformation of the data, as well as the data mining and evaluation methods. We also present the characteristics and motivations behind the use of each of these techniques and propose more adequate and up-to-date taxonomies and definitions for intrusion detectors based on the terminology used in the area of data mining and KDD. Special importance is given to the evaluation procedures followed to assess the detectors, discussing their applicability in current, real networks. Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita [6] In this paper, we provide a structured and comprehensive overview of various facets of network anomaly detection so that a researcher can become quickly familiar with every aspect of network anomaly detection. We present attacks normally encountered by network intrusion detection systems. L. Buczak, Erhan Guven [7] Papers representing each method were identified, read, and summarized. Because data are so important in ML/DM approaches, some well-known cyber data sets used in ML/DM are described. The complexity of ML/DM algorithms is addressed, discussion of challenges for using ML/DM for cyber security is presented, and some recommendations on when to use a given method are provided.

III. METHODOLOGY

We present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. We mainly focus on data reliability protection; give an identity-based cumulative signature design with a designated verifier for wireless sensor networks. According to the advantage of cumulative signatures, our design not only can remain data reliability, but also can condense bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based cumulative signature idea is strictly presented based on the computational Diffie-Hellman statement in random oracle form.

IV.EXPERIMENTAL RESULTS

STP proof generation and STP claim and verification. The two phases and the major communication steps involved. When collects STP proofs from his/her co-located mobile devices, we say an STP proof collection event is started. An STP proof generation phase is the process of the getting an STP proof from one witness. Therefore, an STP

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

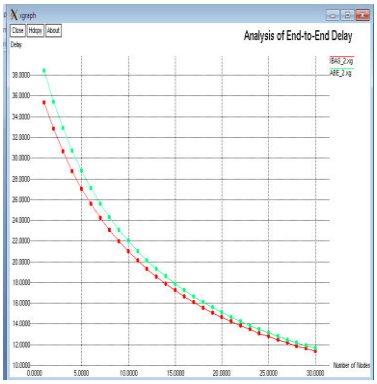
| DOI:10.15680/IJIRSET.2022.1109018 |

proof collection event may consist of multiple STP proof generations. The finally stores the STP proofs he/she collected in the mobile device. A part of the verification job has to be done by CA. Therefore, communication between the verifier and CA happens in the middle of the STP claim and verification phase. The two arrowed lines in red color represent the latter two stages of the Bussard-Bagga protocol. These stages require multiple interactions between the two involved parties, and thereby are represented by doubly arrowed lines. Data Mining also known as Knowledge Discovery in Databases, refers to the nontrivial extraction of implicit, previously unknown and potentially useful information from data stored in databases. Data Cleaning: Data cleaning is defined as removal of noisy and irrelevant data from collection. The Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. In contrast to most existing location proof systems which rely on infrastructure like wireless APs, STAMP is based on co-located mobile devices mutually generating location proofs for each other. This makes STAMP desirable for a wider range of applications. The exact location of such trusted wireless AP is known. In these scenarios, the can send all to CA or skip using CA since the proofs are already trusted. The first model fits well for incognito trusted mobile users while the other model serves well for wireless APs. Trusted Mobile Users: In first case, the trusted witness is not readily recognized.

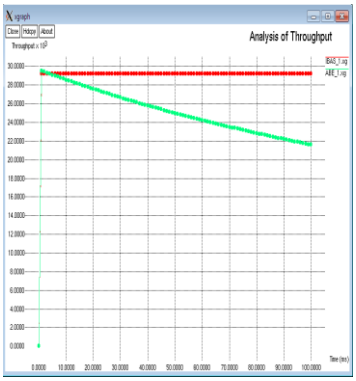
TABLE REPRESENTATION

Packet	Start	End	Values
Packet Size	1000	2000	1234
Transmission Speed	60	65	62
Node Strength	100	200	124
Mobility Range	250	500	258
Average Delay	5	15	6
Time Interval	5	8	7

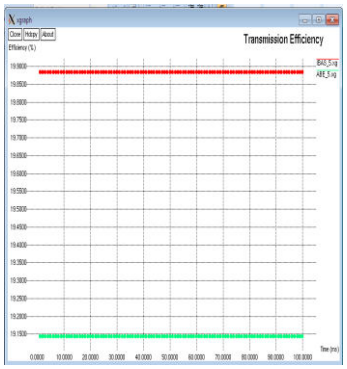
CHART FOR THE TABLE REPRESENTATION



(a)



(b)



(c)

VI. CONCLUSION

This paper we have presented STAMP, which aims at providing security and privacy assurance to mobile users' proofs for their past location visits. STAMP relies on mobile devices in vicinity to mutually generate location proofs or uses wireless APs to generate location proofs. Integrity and non-transferability of location proofs and location privacy of users are the main design goals of STAMP. We have specifically dealt with two collusion scenarios: P-P collusion and P-W collusion. To protect against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the design of STAMP. To detect P-W collusion, we proposed an entropy-based trust model to evaluate the trust level of claims of the past location visits. Our security analysis shows that STAMP achieves the security and privacy objectives. Our implementation on Android smart phones indicates that low computational and storage resources are required to execute STAMP. Extensive simulation results show that our trust model is able to attain a

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109018 |

high balanced accuracy with appropriate choices of system parameters Due to the limited resources of sensor nodes in terms of computation, memory and battery power, secure and energy save data aggregation methods should be designed in WSNs to reduce the energy cost of data collection, data processing and data transmission. In this paper, we present an ID-based aggregate signature scheme for WSNs, which can compress many signatures generated by sensor nodes into a short one. It can reduce the communication and storage cost. Moreover, we have proved that our IBAS scheme is secure in random oracle model based on the CDH assumption, and we also have proved that our aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid. In our future work, we will focus on designing more efficient data.

REFERENCES

[1] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proc. ACM HotMobile*, 2009, Art. no. 3.

[2] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in *Proc. ACM GIS*, 2010, pp. 23–32.

[3] Z. Zhu and G. Cao, "Towards privacy-preserving and colluding-resistance in location proof updating system," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 51–64, Jan. 2011.

[4] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM WiSe*, 2003, pp. 1–10.

[5] R. Hasan and R. Burns, "Where have you been? secure location provenance for mobile devices," *CoRR* 2011.

[6] B. Davis, H. Chen, and M. Franklin, "Privacy preserving alibi systems," in *Proc. ACM ASIACCS*, 2012, pp. 34–35.

[7] I. Krontiris, F. Freiling, and T. Dimitriou, "Location privacy in urban sensing networks: Research challenges and directions," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 30–35, Oct. 2010.

[8] Y. Desmedt, "Major security problems with the 'unforgeable' (feige)- fiat-shamir proofs of identity and how to overcome them," in *Proc. SecuriCom*, 1988, pp. 15–17.

[9] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Security and Privacy in the Age of Ubiquitous Computing*. New York, NY, USA: Springer, 2005.

[10] B. Waters and E. Felten, "Secure, private proofs of location," Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.

[11] C. Chen, C. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," *Information Sciences,* vol. 275, no. 11, pp. 314-347, 2014.

[12] D. Takaishi, H. Nishiyama, N. Kato and R. Miura, "Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks," *Emerging Topics in Computing IEEE Transactions on,* vol. 2, no. 3, pp.388-397, 2014.

BIOGRAPY

Dr.V.Vijayadeepa received her B.Sc degree from university of Madras and M.Sc degree from Periyar University. She has completed her M.Phil at Bharathidasan University. She has awared Ph.D by Anna University, Chennai. She is having 20 years of experience in collegiate teaching and She is the HoD of Department of Computer Application and Head of Student Progression in Muthayammal college of Arts and Science affiliated by Periyar University. Her main research interests include personalized Web search, Web Mining, Web information retrieval, data mining, and information systems.

Ms. V. Thilagavathi completed B.Sc (Computer Science) degree from Muthayammal memorial college of Arts & Science, Periyar University and M.Sc(Computer Science) degree from Muthayammal College of Arts & Science. Presently doing M.Phil Computer Science in Muthayammal College of Arts & Science, Periyar University.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details

TASK ALLOCATION AND RESOURCE SCHEDULE AND FAIRNESS FIRE ALGORITHM IN CLOUD COMPUTING

S. Dharmaraj[*] Dr. P. Kavitha[#]
[*]Head & Assistant Professor of Computer Application
Loyola College, Vettavalam, Tiruvannamalai.india

[#]Assistant professor
Department Of Computer application,
Research and Development,
Muthayammal College of Arts and Science, Namakkal,india

ABSTRACT

The cloud computing has become significant part of day to day life. It is assimilated the several resource for the user's requirement. However, the scale and highly dynamic environment of cloud application executes significant new challenges to resource management and efficient resource scheduling are highly demanded. The problem of Resource scheduling and Task allocation is an important aspect on the cloud performance The propose a systematic approach to denote the reliability, running time, and failure processing of resource scheduling in cloud computing. The Resource Shortest Scheduling and Fairness Fire Algorithm (RSSFFA) is enhance the resource scheduling and task allocation during the time of loading the server in polynomial time and consume an execution time.

Keywords: Cloud Computing (CC), RSSFFA, Task allocation, Resource scheduling, virtual Machine, execution time, utilization, Quality of service (QoS).

1. INTRODUCTION

A cloud is defined as a place over network infrastructure where information technology (IT) and computing resources such as computer hardware, operating systems, networks, storage, databases, and even entire software applications are available instantly, on-demand service[1]. Its objective is to distribute resources among the cloud users, cloud followers, and cloud vendors[2]. With the exponential growth of cloud computing providing flexible computing resource, more and more cloud applications emerge in recent years.

In cloud computing, resource scheduling is allocating resources to user request over the Internet [3]. The resource scheduling has represent jobs, virtual machines and physical machines[4]. The resource scheduling process is highly complex due to the following reasons:

First, the resources accommodated underneath of cloud computing have compound provisioning, configuration, and deployment requirements[5]. Traditional approaches cannot be easily applied in modeling dynamic resource scheduling process due to the variation of system and user requirements.

Second, cloud computing is dynamic because its resources and services can be automatically selected at run-time based on specific requests, and resource in cloud application may be vulnerable to ambiguous factors, such as server failure, malicious threats, the failure of cloud service, etc. It is difficult to plan resource scheduling approach at the design time for all dynamic performances during the execution, which leads to a loss of reliability mechanism.

Third, many applications, e.g., financial transactions and scientific computing, are real-time in nature, where the correctness depends not only on the computation results, but also on the time instants at which they become available. It is essential to preserve the ability to provision virtual machine within the deadline.

Finally, the characteristics of cloud computing, such as rapid elasticity and multitenant, bring about many stimulating confirmation provides which have deep impact on the concert of system. Most efforts to authenticate mechanisms cannot be approximately possible to confirm the precision of adaptive resource scheduling strategy.

This paper investigate improvement of cloud technology and the extensive deployment of cloud platforms, the problem of resources scheduling and task allocation in cloud computing. The proposed The Resource Shortest Scheduling and Fairness Fire Algorithm (RSSFFA) that performs resources scheduling and allocates task efficiently in cloud computing environments.

2. LITERATURE SURVEY

This section provides a brief review of resource scheduling and task allocation strategies. Many researchers have proposed solutions to overcome the problem of resource scheduling and task allocation.Tsai J-T et al[6] proposed by a multi-object approach that employs the improved differential evolution algorithm. This existing method provides a cost and time model for cloud computing. Cheng C et al[7] describe a load balancing and scheduling algorithm that does not consider job sizes. L. Wei et al[8] expounded on the heterogeneous Resource Allocation (RA) in the IaaS cloud. The recommended algorithm incorporates a VM allocation that guarantees the proper distribution of heterogeneous tasks to avoid unnecessary resource deployment and evaluates the number of active PMs. Sun et al[9] proposed a new scheduling mechanism by establishing a multi-for Quality of service (QoS) optimization objective function and combining it with the immune Cologne algorithm, which has significantly improved the problems such as load imbalance and low user experience. J. Lin et al[10] discussed the two-stage RA and task scheduling method in the Cloud Computing environment. However, a major issue is efficient task scheduling and resource allocation between multiple cloud clients and data centers. Gougarzi et al[11] proposed a resource allocation problem that aims to minimize the total energy cost of cloud computing systems while meeting the specified client-level SLAs in a probabilistic sense. To applied a reverse approach that applies a penalty if the client does not meet the SLA agreements. Keshk et al[12] proposed the use of modified ant colony optimization in load balancing. This method improves the make span of a job. This system does not consider the availability of resources or the weight of tasks.

3. CLOUD PLATFORM AND ITS SCHEDULING ISSUES

3.1 Cloud Platform

Cloud computing is known as pay-as-you-go business service model. The most important aspect of cloud computing is its virtualization technology, the boundaries of the cloud computing is permits to split of physical resources from the virtual deployment platform. It can be observed as a network of resource scheduling, and users can simultaneously get resources from the "cloud" and pay for their requirements, In addition, related with the traditional network application model, it also has the characteristics of on-demand deployment, high flexibility, high reliability, and cost-effectiveness.

3.2 Resource Scheduling and Task allocation problem in Cloud Computing

The scheduling problem in cloud computing is an NP-Hard problem, which can be divided into two categories: task allocation and resource scheduling.

Task allocation is to dynamically assign tasks based on the workload of the server so as to achieve scheduling goals such as load balancing and cost-effectiveness. Resource scheduling is to dynamically allocate resources to users by responding to their needs and following certain rules. Resource scheduling is not necessarily fair, and it needs to set scheduling goals based on specific application scenarios. In general, both scheduling issues exist in a cloud service, but task scheduling is more important. Because task scheduling can actively select nodes with suitable resources to execute tasks, while resource scheduling is reactive and is forced to start when a node is found to be under-resourced during task execution. Therefore, a reasonable task scheduling strategy not only improves the user experience, but also keeps the cloud resources at a high utilization rate in the long run, avoiding idle and wasteful resources.

3.3 Resource Shortest Scheduling and Fairness firefly algorithm (RSSFFA)

The proposed Resource Shortest Scheduling and Fairness Firefly Algorithm (RSSFFA) improves cloud user satisfaction, and it takes the minimum delay time to solve a resource scheduling and task allocation problem. First, the cloud model uses firefly algorithms to find a better solution for resource task scheduling based on a strong global search. Then, the first pheromone improves firefly algorithm scheduling and improves optimal global solutions in cloud computing.

Algorithm Steps

Input: Task length T_l

Output: Evaluate task length density D_T

Begin

Import Task length T_{li} , i=1, 2,…n

Objective functions$f(x), x = (x_1, \dots, x_d)^T$

Generate early firefly population$X_i (i = 1,2, \dots, n)$

The Light density of$l_i at X_i is determined by f(X_i)$

Define absorbance factorγ

While $(t > MaxGeneration)$

For $i = 1$: $allnfireflies$

For $j = 1$: $iallnfireflies$

if $(I_j > I_i)$

Move firefly i to j in d dimension

End if

$Attractivenessvarieswithdistancervia \exp[-\gamma r]$

Evaluate new solutions and update light intensity

End for j

End for i

$Rankthefireflies and find the current best$

End while

$post - processresults and visualization$

End

Return $\leftarrow D_T$

Stop

The main purpose of the RSSFFA is to achieve better resource utilization performance and task response time. This algorithm estimates the calculated share of each Virtual Machine based on the set of tasks. This Resource Shortest Scheduling and Fairness Firefly Algorithm (RSSFFA) algorithm enhances resource utilization performance and minimizes execution time costs better than existing methods.

In Figure 1: the architecture of the proposed diagram for resource allocation and scheduling performance. Due to many cloud users, the user loads different workflow functions, dependencies, and data transfers.

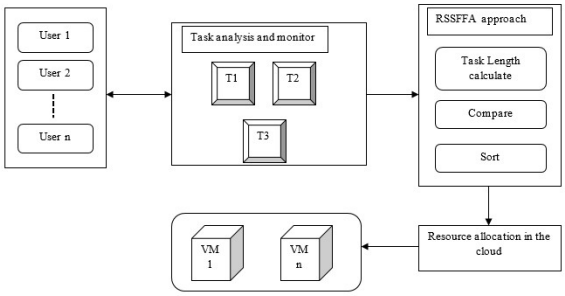


Figure 1. Proposed diagram for RA scheduling in cloud computing

3.5 Resource allocation in virtualized cloud

It is the process of resolving the imbalanced task scheduling load of the virtual machine. The Resource Shortest Scheduling and Fairness Firefly algorithm (RSSFFA), not only to shorten tasks, has been proposed to maintain the load balancing of virtual machines in the data center. The RSSFFA algorithm retains better performance and load balancing features than other scheduling strategies.

Input: Task fitness function $\overrightarrow{\beta_{ij}}$

Output: Resource allotted (R_a) based on task fitness

Begin

For all tasks $\overrightarrow{\beta_{ij}}$ in the scheduled task list

For all resources Rj

Calculate CTij = ETij + RTj

End

End

Do until all tasks in the scheduling-Tasks List are workflow.

Resource, R1 Find the minimum execution time, task Tk and least completion time.

When the resource R1 is busy

Then

The next resource is the next least completion time and finds R1.

Go to

Else

Resource, Execute R1 Task Tk

End if

TK of the task removed from the scheduled task list

Update RTL

Update CTil for all I

End do

Return $\leftarrow R_a$

This algorithm provide the task assigned in the cloud environment efficiently. Where R1 refers to Resource Variable, Tk denotes Execute task, CT refers to computing time, ET presents End Time, and R1 refers to resource time. Scheduling the workflow task list, a resource to system execution for data allocation, and calculating the computing time for the support and end time until the R1 resource is busy will continue in another workflow process. The next process takes a minimum completion time for the resources, and finally, the Scheduling resource task evaluates and updates all jobs.

4. ANALYSIS TECHNIQUES

To analysis the resource scheduling and Task allocation performance in the cloud environment using Network Simulator version 2 (NS2) on the Windows operating system. To evaluate resource allocation performance based on Quality of service (QoS) parameters, which are scheduling performance, migration time, resource utilization, and time complexity, to achieve better performance.

Table 1. Details of Parameters Processing

Parameters used	Values
Input data	Workflow scheduling data
Simulation Language	Network Simulator (NS2)
No of nodes	100
Number of tasks	10-50

Table 1 shows the process's defined values and analysis parameters. The Resource Shortest Scheduling and Fairness Firefly algorithm (RSSFFA) is calculated No of parameter used in simulating language and task.

Table 2 .Analysis of scheduling performanc

No of task	MMBF in ms	SBA-SO in ms	RSSFFA in ms
10	20	15	10
20	25	20	18
30	30	25	22
40	37	27	25
50	35	31	29

Table 2 describes the scheduling performance, and the scheduling performance is compared with existing algorithms to prove that the proposed algorithm is better than existing algorithms.

Scheduling workflow tasks = Time speed / Performance level *100

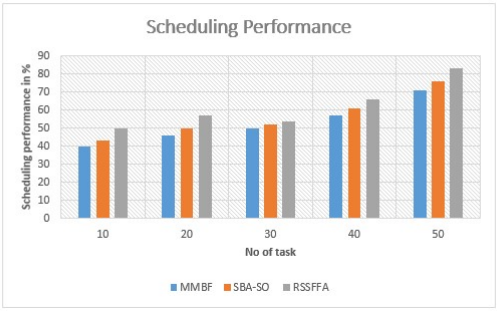


Figure 2. Analysis of scheduling performance

Figure 2 shows the scheduling performance flow values analysis from the existing methods like Min-Min Best Fit (MMBF), which provides 71%, and SBA-SO provides 76%. The proposed RSSFFA implementation produces a higher efficiency of 83% in scheduling values than other methods.

$$M_t = \int \sum_{n=1}^{n} s(s)$$

Let's assume denotes server status, and n refers to the number of servers. In task migration, the task is assigned to the executor server. Perhaps the executor server does the task if the server is idle. If the executor server is busy performing the prior task, the present task is migrated to another executor server to perform the task. The equation below calculates the migration time to switch the task from one executor server to another.

Time complexity is low, and the proposed algorithm achieves low time complexity performance

Time complexity T (n) = n - 1 ≤ 1, n when n ≥1

Table 3. Time complexity

No of task	MMBF in %	SBA-SO in %	RSSFFA in %
10	40	43	50
20	46	50	57
30	50	52	54
40	57	61	66
50	71	76	83

Figure 3. Describes time complexity performance for resource scheduling and task allocation

in cloud computing using RSSFFA. The proposed RSSFFA algorithm time complexity performance is 29 ms; likewise, the existing Min-Min Best Fit (MMBF) algorithm is 35 ms, and the SBA-SO time complexity performance is 31 ms.

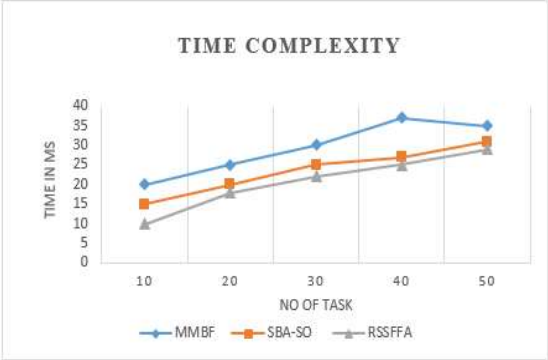


Figure 3. Time complexity

5. CONCLUSION

The propose Resource Shortest Scheduling and Fairness Firefly Algorithm (RSSFFA) solves the task scheduling problem with the minimum delay time and improves user satisfaction. The RSSFFA algorithm improves the best solution for task scheduling in cloud computing. The firefly algorithm has a minimum running time of job submission. The proposed algorithm can be used as a predictive model for efficiently allocating resources in cloud computing mode within actual time. It produces scheduling performance of 83%, Virtual Machine migration time of 8 seconds, time complexity performance of 29 ms, and resource utilization performance of 82.9%. The proposed RSSFFA algorithm performs better with a lower time complexity than the existing algorithms.

REFERNCES

1 S. S. Manvi, G. K. Shyam. Resource management for Infrastructure as a Service (IaaS) in cloud computing: a survey. *Journal of Network and Computer Applications,* 2014, **41**(0): 424-440.

2 A. G. Kumbhare, Y. Simmhan, M. Frincu, V. K. Prasanna. Reactive resource provisioning heuristics for dynamic dataflows on cloud infrastructure. *IEEE Transactions on Cloud Computing*, 2015, **2**(2): 105-118.

3 H. Zhao, M. Pan, X. X. Liu, et al. Optimal resource rental planning for elastic applications in cloud market. *Proceedings of the 26th International Parallel & Distributed Processing Symposium. IEEE Computer Society Washington, DC, USA*, 2012: 808 - 819.

4 L. Liu, M. Zhang, Y. Lin, L. Qin. A survey on workflow management and scheduling in cloud computing. *Proceedings of the 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Computer Society, Washington, DC, USA*, 2014:837-846.

5 H. Zhang, B. Li, H. Jiang, F. Liu, et al. A framework for truthful online auctions in cloud computing with heterogeneous user demands. *Proceedings of the 32st Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE Computer Society, Washington, DC, USA,* 2013: 1510-1518.

6. G. Jung, K. M. Sim. Agent-based adaptive resource allocation on the cloud computing environment. *Proceedings of the 40th International Conference on Parallel Processing Workshops. IEEE Computer Society,Washington*, DC, USA, 2011: 345-351.

7.Cheng C, Li J, Wang Y , An energy-saving task scheduling strategy based on vacation queuing theory in cloud computing. *Tsinghua Sci Technol* **20**(1):28–39

8.W. Wei, X. Fan, H. Song, X. Fan and J. Yang, "Imperfect Information Dynamic Stackelberg Game Based Resource Allocation Using Hidden Markov for Cloud Computing," *IEEE Transactions on Services Computing,* **11**(1), pp. 78-89, 1 Jan.-Feb. 2018.

Doi: 10.1109/tsc.2016.2528246.

9. Singh P, Dutta M, Aggarwal N. A review of task scheduling based on meta-heuristics approach in cloud computing. *Knowledge and information systems,* 2017, **52**(1): 1-51.

10.J. Lin, D. Cui, Z. Peng, Q. Li and J. He, "A Two-Stage Framework for the Multi-User Multi-Data Center Job Scheduling and Resource Allocation, *IEEE Access,* **8,** 19863-197874, 2020,

Doi: 10.1109/access.2020.3033557.

11. Goudarzi H, Ghasemazar M, Pedram M, Sla-based optimization of power and migration cost in cloud computing. *In Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, 2012: 172-179.

12. Keshk AE, El-Sisi AB, Tawfeek MA Cloud task scheduling for load balancing based on intelligent strategy. *Int J Intell Syst Appl* 2014 **6**(5):25-30.

Received: 24 May 2022 | Revised: 4 July 2022 | Accepted: 16 July 2022

DOI: 10.1002/ett.4619

SPECIAL ISSUE ARTICLE

WILEY

Medical data quality management using butterfly optimization with adaptive threshold sensitive energy-efficient routing protocol and multidimensional chaotic blowfish encryption in wireless body networks

M. Santhalakshmi[1] | **P. Kavitha**[2]

[1]Department of Computer Science, Sri Kailash Women's College, Attur, India

[2]Department of Computer Applications, Muthayammal College of Arts & Science, A Unit of Vanetra Group, Rasipuram, India

Correspondence
M. Santhalakshmi, Department of Computer Science, Sri Kailash Women's College, Attur, India.
Email: santhares12@gmail.com

Abstract

Nowadays, medical applications require much medical information to analyze various diseases. To collect various medical data, wearable devices collect patient health and medical details using a wireless body area network. The collected details consist of several critical details: oxygen level, heart attack information, blood pressure, airflow and so forth. These details are broadcast to the healthcare centers using wireless technologies to make clinical decisions. During medical information transfer, the data quality and critical events are difficult to maintain because it reduces the packet delivery, transmission delay, and high energy. So, this article introduces bacterial optimization and adaptive threshold-sensitive energy-efficient routing protocol (BOATSEE) to transmit the medical data. The method aggregates the sensitive data by selecting the cluster head and effectively broadcasts the critical data. In addition, the optimized method manages the network lifetime and energy using an energy-efficient method. Also, we have proposed a multidimensional chaotic blowfish encryption (MCBE) algorithm to enhance the system's security. Then the system's efficiency is computed based on metrics like energy consumption, packet delivery ratio, end-to-end delay, and QoS metric-associated restraints. The results reveal that the proposed system is efficient in managing the medical data quality with minimum energy utilization, packet loss rate, delay, and maximum packet delivery ratio when compared with the conventional approaches. Our method also proved to be more secure than the traditional systems.

1 | INTRODUCTION

Wireless body area networks,[1] also called body sensor networks, consist of several wearable devices that monitor patient health remotely. The wearable devices are placed in fixed positions such as bags, hands, packets, wrist and so forth.[2] The sensor devices have a body sensor unit and larger smart devices to ensure the interface between the patient and applications. The devices are connected via gateway technologies to transmit information from one place to another. Sensors that run in low-power mode and have no configuration interfaces are common in the Internet of Things (IoT). An IoT gateway is typically used to send and receive data from and to these IoT sensors or devices. Devices, cameras,

equipment, and software may communicate via an IoT gateway with the cloud. An IoT smartphone app may be a quick and easy way to link these devices. According to the communication technologies, medical records are transmitted via the internet; also, patient location is independent. The body sensor network is less expensive and can monitor patient health information with minimum effort and complexity.[3] The physiological sensor information is combined to assist the patients and rehabilitated according to their health condition. The external processing components help broadcast the information to healthcare centers worldwide.[4] The gathered information is processed in the end-unit using computerized technologies, and if emergency data is identified, the alarm is ringed to alert the patients.

However, wearable technologies meet the data quality issues[5,6] because clinical decisions are based on the collected information. Therefore, the body sensor networks give important attention while gathering information, and the information quality is sustained only by proper management. The sensor gathers a huge volume of data that helps analyze the patient's health conditions faster and accurately.[7] The invalid sensor may affect the data quality; the limited power reserves, unreliable network links, and inherent communication affect the entire data collection process. The unreliable and invalid sensor increases[8] the false alarm rate and weakens software/hardware design. The security factor also affects the data quality and reduces the decision-making accuracy. The third-party influences sensor data transmission, reducing communication rate, security, integrity, authentication, confidentiality, and computational capability.[9,10] In addition, body sensor networks face an invasion of privacy, interference, and cost issues while remotely analyzing patient health.

To overcome this research issue, bacterial optimization and adaptive threshold-sensitive energy-efficient routing protocol are applied in this work. The method predicts the broadcasting route according to the node energy consumption.[11,12] Once the node consumes minimum energy value, it has been utilized for further data transmission. The body sensor networks transmit the sensitive data; therefore, the transmitting clustering head has been selected based on the bacterial optimization technique. The optimization process manages the network energy and lifetime while selecting and forming the cluster. This process identifies the optimized route, reduces packet loss, and maintains data quality. Health care organizations may gather, store, organize, evaluate, and optimize patient treatment records and other important data using a healthcare information system. Community health patterns and other macro-environmental data may be readily accessed using these platforms. The system's effectiveness is evaluated using the NS2 simulation tool with respective parameters.

The main contribution of this study

i. Designing the proposed system security might be improved by using the MCBE algorithm.
ii. An adaptive threshold-sensitive energy-efficient routing protocol (BOATSEE) is introduced in this research to transport medical data.
iii. The approach successfully broadcasts the vital data and aggregates the sensitive information by picking the cluster head.
iv. An energy-efficient approach is used to control the network lifespan and energy consumption in the optimized method.
v. Metrics including energy consumption, packet delivery ratio, end-to-end latency, and QoS metrics-associated restrictions are used to calculate the system's efficiency.

The further part of the article is arranged as shown, Section 2 discusses the different researcher's works on wireless body area network-based data transmission. Section 3 explains bacterial optimization's working process and adaptive threshold-sensitive energy-efficient routing protocol. Section 4 explains the mechanism of the multidimensional chaotic blowfish encryption (MCBE) algorithm. Section 5 investigates the introduced system's efficiency, and the conclusion is summarized in Section 6.

2 | RELATED WORKS

Huzooree et al[13] maintain data quality and reliability while monitoring diabetic patient health using body sensor networks. This work uses the data quality dimension framework to manage the sensor information. The sensor information was investigated at in-network, sensor, and human-centric levels with high precision and accuracy. As part of this study, we will look at the issue of ensuring the greatest dependability in the transmission of data from a defined source to an identified destination through a single channel. There is no guarantee that the subpaths of a perfect path are also perfect in this issue of route selection and routing. This pre-calculation is important when various quantities of data need to be communicated at different times.

Ventura et al[14] apply the priority queue-based data transmission (PQDT) in the body area network to resolve the quality issues. This study's main intention is to manage the energy factor, reliability, and end-to-end delay problem when transferring collected sensor information from one place to another. The transmitted data priority is investigated for every transaction to reduce data loss and increase data quality and reliability.

Goyal et al[15] introduced the time-domain based delay-sensitive energy effective protocol (TDSEE) to maintain the data quality in BSNs. The sensor devices collect physiological information like ECG, EEG, and normal health information. The gathered information is investigated to identify the normal and emergency data. After that, a sensitive medium access control protocol broadcasts the information. This process reduces the unwanted emergency problem also increases the data transmission rate.

Ullah et al[16] recommend a fog-assist link aware energy protocol (LAEEBA) to broadcast the sensor information. The system intends to reduce the latency issues by applying the LAEEBA method. The method transmits the information after computing the network and node energy factor, which helps attain effective data transmission, and the introduced method dies after completing the 7445 rounds. This process increases the data transmission rate and minimizes the delay (2 s) compared to existing methods.

Ullah et al[17] introduced the traffic priority-delay aware routing protocol to perform the sensor data transmission. This process aims to increase the data transmission by maintaining high residual energy. The sensor information is classified into emergency, normal, on-demand, and high threshold data. Then transmitting path is selected by examining the energy factor. Afterwards, the shortest path is chosen from the minimum energy value. Finally, on-demand analysis is applied to predict the network traffic. This process helps to improve the data transmission rate.

Kour et al[18] apply an energy-efficient routing protocol in WBANs to minimize packet loss and maximize the network throughput. The distance vector routing protocol is initially applied to identify the shortest path between source and destination. Then, a secure and energy-aware protocol is utilized to recognize the network energy value and minimize data loss. Thus the procedure enhances the entire data transfer rate and throughput and reduces the packet loss. According to the various researchers' opinions, the wireless body sensor networks played an important role while remotely monitoring patient health. Several routing protocols are utilized to reduce the data loss between source and destination. However, data quality and reliability are the main factors when performing data broadcasting. Therefore, this work utilizes optimization techniques with a routing protocol to enhance the overall data transfer and reduce packet loss. The major contributions of this research include:

- The energy-aware routing protocol is used to manage data quality, reliability, and critical data transmission in wireless body area networks.
- To enhance the security of sensitive medical data by using the encryption and decryption algorithm.

3 | BACTERIAL OPTIMIZATION ALONG WITH ADAPTIVE THRESHOLD SENSITIVE ENERGY EFFICIENT ROUTING PROTOCOL

This work's primary objective is to manage data quality, reliability, and critical data transmission in wireless body area networks. Existing methods consume high packet loss and failure to manage the system reliability. Therefore, an optimized bacterial optimization algorithm with routing protocols is introduced to overcome the research problem. The overall working process of the wireless body area network-based data quality transmission process is illustrated in Figure 1.

Initially, packet loss has been reduced when transferring sensitive information from sender to receiver. This is achieved by choosing shorts and a high residual energy consumption network path. The adaptive threshold sensitive energy efficient routing protocol is utilized to identify critical and periodic data transmission paths. The short path is identified by forming the cluster, and the cluster head is selected in the first and second levels. Improve the network's lifespan primarily through inventing routing methods that provide reliable communication while using less energy. Clustering sensor nodes (SNs) has been generally regarded as an essential strategy for extending the life of wireless sensor networks (WSNs) life. Many academics have been working on ways to extend the network's life. The most important component in extending the life of a network is reducing energy usage. Multi-objective optimization is the method put out by the authors of this research. Once the cluster head is selected, user attributes are selected to broadcast the information securely. The CH transmits the attribute values, soft threshold (ST), count time (CT), and hard threshold (HT) values to the user. The schedule is allocated for CH when the sensed information is more than the HT value, stored in the SV (internal value).

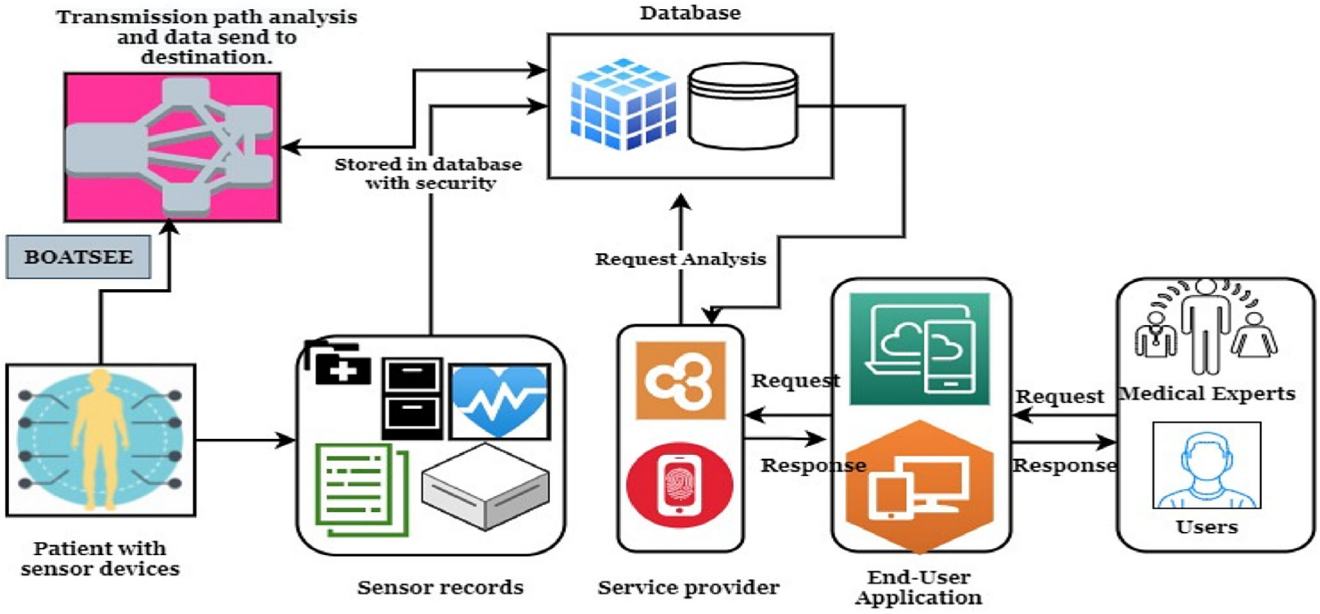


FIGURE 1 WBAN data transmission architecture

Setting all coefficients with absolute values less than or equal to the threshold is known as hard thresholding. Another technique is soft thresholding, which first reduces the absolute values of nonzero coefficients until they are equal to zero.

During this process, every node does not have the same number of sensor nodes. Therefore the clusters are formed according to the data aggregation. The aggregated data is broadcast to the base station by analyzing the cluster information. Suppose the nodes are presented in the range, and the sensed data has been transmitted successfully by forming the pair. After that, only one pair node is selected to broadcast the information; the remaining nodes fall under the sleeping style. Then the active nodes are selected according to the response, and sleeping style nodes are considered inactive or sleep nodes. The cluster head (CH) is selected based on the bacterial optimization algorithm to choose the optimized node using the food searching process. Therefore, the protocol effectively provisions persistent, historical, and on-time queries because of the continuous learning and searching process. The base station responds to the query after obtaining data from the cluster head. The request is processed according to the cluster members because high members consume more time to complete the data transmission process. If the node receives the critical or emergency data, it has been broadcast to CH according to the periodic interval. The selected interval does not surpass the threshold, and the periodic critical information transmission is updated continuously to improve the data transmission rate. Then the overall clustering and shortest path selection process are illustrated in Figure 2.

Then, the path reliability value should be detected to improve the overall data broadcasting. The source-destination path reliability is computed using Equation (1).

$$\boldsymbol{Re}_{\text{path}(\boldsymbol{i},\boldsymbol{Dis})} = \boldsymbol{Re}_{\text{link}(\boldsymbol{i},\boldsymbol{j})} * \boldsymbol{Re}_{\text{path}(\boldsymbol{j},\text{Dist})}. \tag{1}$$

For transmitting sensed data from source node $\boldsymbol{i}$ to destination node $\boldsymbol{Dis}$ by computing path reliability $\boldsymbol{Re}_{\text{path}(\boldsymbol{i},\boldsymbol{Dis})}$. The reliability of a network is a measure of how long it can operate uninterrupted. Several equations are used to gage a system's reliability. There are two types of MTBF: the total service time and the number of failures. The reliability is computed from two nodes $(\boldsymbol{i},\boldsymbol{j})$ and identified path distance $\boldsymbol{Re}_{\text{path}(\boldsymbol{j},\text{Dist})}$. Along with this, node reliability is estimated using Equation (2).

$$\boldsymbol{Re}_{\text{link}(\boldsymbol{i},\boldsymbol{j})} = (\mathbf{1} - \propto)\boldsymbol{Re}_{\text{link}(\boldsymbol{i},\boldsymbol{j})} + \propto \boldsymbol{X}_{\boldsymbol{i}}. \tag{2}$$

Node reliability is computed with the help of two nodes link reliability $\boldsymbol{Re}_{\text{link}(\boldsymbol{i},\boldsymbol{j})}$ with node average weight factor $(\mathbf{0} < \propto \leq \mathbf{1})$ and average probability value of the transactions $\boldsymbol{X}_{\boldsymbol{i}}$ is estimated in Equation (3).

$$\boldsymbol{X}_{\boldsymbol{i}} = \frac{\boldsymbol{N}_{\text{acks}}}{\boldsymbol{N}_{\text{Trans}}}. \tag{3}$$

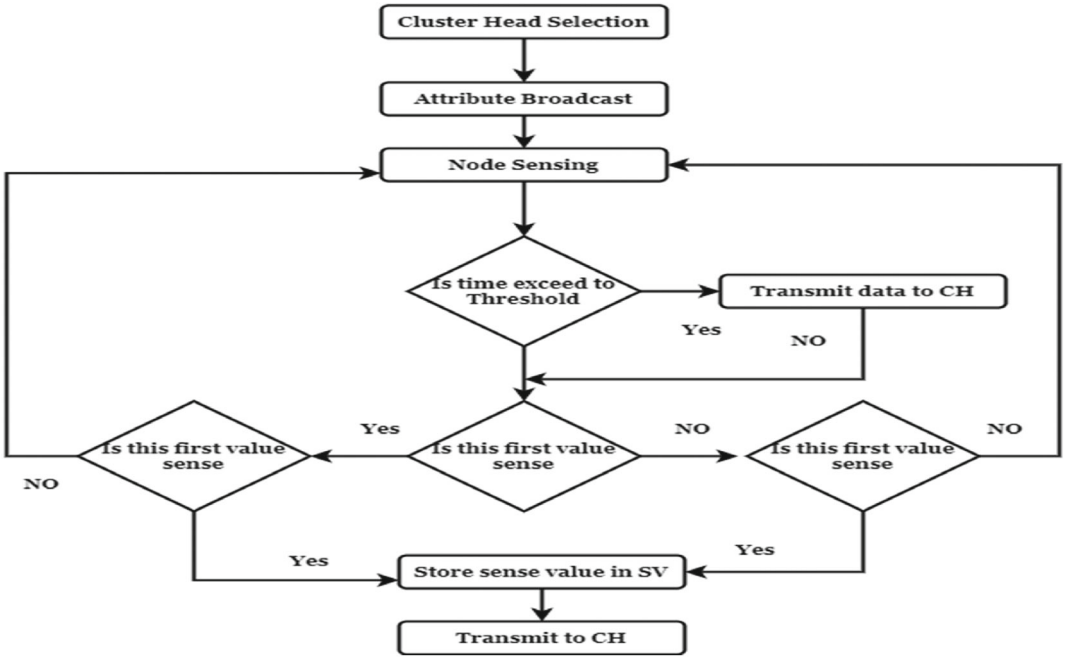


FIGURE 2 Adaptive thresholding based route selection clustering process

When data from the cluster sensors is collected and sent to the base stations via the cluster head, a node in the network. The base station receives data from sensors in its cluster via this node. During this computation, $\propto$ taking the value as 0.4 and the transaction probability value is estimated by taking the ratio of the count of received packets acknowledgement ($\boldsymbol{N}_{\text{acks}}$) and the number of the packet transmitted ($\boldsymbol{N}_{\text{Trans}}$). As said earlier, the cluster head is selected according to the butterfly optimization approach, which helps maintain the network lifetime and energy factor. The algorithm works according to the fragrance $\boldsymbol{fr}$ and stimulus intensity **SI** characteristics. Each node is connected according to the **SI** value with the respective objective function. The $\boldsymbol{fr}$ value is derived from the **SI** that is computed using Equation (4).

$$\boldsymbol{fr} = \boldsymbol{smSI}^{\boldsymbol{e}}. \tag{4}$$

This computation utilizes the sensory modality $\boldsymbol{sm}$ and exponent-dependent modality values; these values come from (0, 1). The effective cluster head is selected according to the initialization, iteration, and final phase. Initially, every node (butterfly)'s fitness value should be estimated in the given space. The cluster head is selected according to the global search process defined in Equation (5).

$$\boldsymbol{b}_{\boldsymbol{u}}^{\boldsymbol{it+1}} = \boldsymbol{b}_{\boldsymbol{u}}^{\boldsymbol{it}} + \left(\boldsymbol{rnd}^{\boldsymbol{2}} * \boldsymbol{h}^{*} - \boldsymbol{b}_{\boldsymbol{u}}^{\boldsymbol{it}}\right) * \boldsymbol{fr}_{\boldsymbol{u}}. \tag{5}$$

The butterfly moves in the search space and the optimized solutions $\boldsymbol{h}^{*}$ is computed from the solution vector $\boldsymbol{b}_{\boldsymbol{u}}^{\boldsymbol{ilt}}$ in $\boldsymbol{it}$s iterations. Here, (0, 1) random number is utilized to derive the fragrance of the node. The butterfly can produce a strong scent. The butterfly's health and well-being are also linked to the scent. As a result, the fitness of a butterfly will change as it goes from one location to another in the search area. Now, the scent that butterflies detect is transmitted across long distances to all other butterflies in the area. Using metaheuristics, the butterfly optimization algorithm (BOA) simulates butterflies' mating and foraging behaviors. BOA has been upgraded in this study with three new algorithms that prevent it from becoming stuck in local optima and have a nice mix of exploration and exploitation capabilities. For all the computations, the current solution is obtained using Equation (6).

$$\boldsymbol{b}_{\boldsymbol{u}}^{\boldsymbol{it+1}} = \boldsymbol{b}_{\boldsymbol{u}}^{\boldsymbol{it}} + \left(\boldsymbol{rnd}^{\boldsymbol{2}} * \boldsymbol{b}_{\boldsymbol{v}}^{\boldsymbol{it}} - \boldsymbol{b}_{\boldsymbol{w}}^{\boldsymbol{it}}\right) * \boldsymbol{fr}_{\boldsymbol{u}}. \tag{6}$$

Then utilizing the switch probability values, the computed solutions are switched to obtain the exact solution for cluster head selection. Here, the cluster head is selected according to the reliability and energy consumption factor. The node

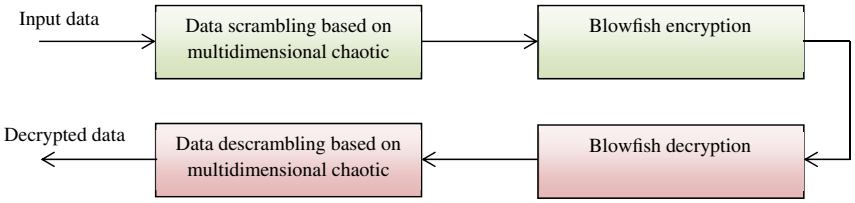


FIGURE 3 Representation of the encryption and decryption process using the proposed blowfish

with a high residual energy value is chosen as the cluster head with respective criteria. From the selected shortest path, data has been transmitted successfully with minimum packet loss, delay, and maximum packet delivery rate. Next, the efficacy of the platform is computed in the following section. Point-to-point data streams or channels are used for this transmission. Wireless networks are becoming more common for these channels, which may have historically been made of copper lines.

4 | MULTIDIMENSIONAL CHAOTIC BLOWFISH ENCRYPTION

Blowfish is an 8-byte block symmetric block cipher that encrypts data. There are two aspects to the blowfish algorithm: data encrypting and key extension. The expansion of the key transforms a variable-length key of up to 64 bytes into 4168-byte arrays of subkeys. The blowfish algorithm works with a wide range of subkeys, which are precomputed before any data encrypting and decrypting. Blowfish is much faster than DES and IDEA, plus its completely open-source, so anybody can use it for whatever they choose. Even still, its limited block size meant it could not replace DES, which is why it was deemed unsafe in the first place. The block size of blowfish is 64 bits, and the key length may range from 32 to 448 bits. In each of the 16 feistel-like rounds, a 64-bit block is divided into two 32-bit words, and each word is processed in turn. Blowfish encrypts and decrypts data using a single encryption key.

Several cryptographic methods have been invented and are widely utilized, including AES, blowfish, RC5, RSA, and IDEA. One key is used to encrypt data in symmetric cryptography, also known as secret-key cryptography. One key is used for encryption and decryption in symmetric cryptography, making it the simplest kind of cryptography to utilize. To decode the data encrypted by the cryptographic technique, someone having access to the secret cipher key must be trusted. While it is possible to employ secret key cryptography on both in-transit and at-rest data, it is more typically used on at-rest data since revealing a recipient's secret might undermine the communication.

In asymmetric cryptography, also known as public-key cryptography, two keys are used to encrypt the data. The encryption key is used to protect the communication, while the decryption key is used to read it. Symmetric cryptography requires two keys to encrypt and decode data, but only one of those keys may be utilized in the encryption process.

Data is protected using hash functions, one-way, irreversible functions, but the original message cannot be recovered. Hashing is a method of transforming a given string into a fixed-length string. The outputs of a good hashing algorithm are unique for each input. The majority of them are employed to store binary information or data. Due to the significant association between pixels, it is difficult to employ explicitly in multimedia information and useless for encrypting color images. The regularity of multimedia medical information is typically high, necessitating real-time interaction. Images are saved and sent through multimedia applications by healthcare workers. They can make a better diagnosis with the use of multimedia. Education and training in medicine can also be accomplished with this technology. It is common for patients to employ multimedia as an educational and rehabilitative aid. Text, data, images, graphics, sound, and video animation may seamlessly integrate into a single digital file using multimedia. There are many innovative approaches to improve the user's experience with information. As a preprocessing stage, a technique based on a multidimensional chaotic map is employed to eliminate the strong relationships among images and enhance the entropy values. The information is scrambled and separated into blocks based on a multidimensional chaotic map, and all these blocks are then sent to the blowfish encryption method. The suggested algorithm's block diagram is shown in Figure 3.

The suggested system's general phases are provided in the Algorithm 1.

Algorithm 1. Data encoding

Input: *Actual data, parameters, and secret chaotic keys*
Output: *Encrypted data*
Start.
Read the input data
Employ the suggested multidimensional chaotic mapping to scramble the data, then split it into eight sub-blocks utilizing the Algorithm 2
Use the Blowfish encryption algorithm to obtain encoded data
Use the Blowfish decryption algorithm to obtain decoded data
Employ the inverse scrambling procedure to retrieve the actual data
Stop.

Data scrambling using multidimensional chaotic map.

When encrypting a medical image, the strong association between pixels and the enormous volume of the data might address the security problem. The data is scrambled depending on the chaotic map in the developed framework by initializing sequence employing multidimensional chaotic mapping to scramble input data, then generating a further sequence using another initial condition of multidimensional mapping and mapping the array of the chaotic map results, splitting the data into eight blocks

The suggested data scrambling depending on the chaotic map is shown in Algorithm 2

Algorithm 2. Data scrambling

Input: *Original data, Data dimensions $n \times m$ Parameters, and Secret Chaotic Keys*
Output: *block j where $j = 1, \ldots, 8$*
Start.
Consider $L = n \times m$
Create random sequence utilizing the multidimensional chaotic map
Standardize the chaotic map array
Resize the data from the multidimensional matrix to a one-dimensional array
Substitute recurring number with the missing number
The data values are scrambled based on array positions
Convert the multidimensional array to a two-dimensional array
Create another random sequence utilizing a chaotic map with another initial condition
Standardize the chaotic map
Split the scrambled data into 8 sub-blocks
Block j where $j = 1, \ldots, 8$ according to the array
Stop.

The decryption algorithm uses the reverse of all stages to retrieve the original data.

5 | RESULT AND DISCUSSION

The effectiveness of the introduced BOATSEE routing protocol dependent sensor information transfer mechanism is presented here. The suggested system is developed using an NS2 simulator with a 4 to 6-m distance hospital scenario. Support for cable and wireless network protocols can be found in network simulator 2 (NS2). It offers a highly flexible foundation for various network parts, protocols, traffic, and routing types to be simulated for wired and wireless simulations. Efficiency considers the amount of time necessary to execute a certain algorithm and the amount of storage space required. An algorithm that seems much more complicated and makes use of both metrics can be more effective. The introduced BOATSEE algorithm efficiency is compared with the existing methods such as PQDT,[14] TDSEE,[15] and LAEEBA.[16] The following simulation metrics are utilized during the implementation as shown in Table 1.

TABLE 1 Simulation metrics

Metrics	Values
Area of simulation	350 m^2
Count of nodes	46 node
MAC	IEEE 802.15.4
Packet size	45 bytes
Broadcast rate	260 kbps
Frequencies band	420 MHz, 868 MHz, 2.4 GHz
Mode of channel	Log shadowing wireless framework
Time of simulation	400 s

A technique for controlling access to sensitive media is employed to disseminate the information. This technique mitigates the unwelcome emergency and accelerates the pace at which data may be sent. The information is sent by the technique after the network and node energy factor has been computed, contributing to the successful data transmission completion. The method that was introduced expires once it has completed 7445 cycles. Depending on the simulation metrics, in this work, efficiency is computed utilizing various metrics like end-to-end delay, energy utilization, packet loss, and packet delivery rate. The computed metrics are provided in Table 2.

Based on the above performance metrics, the obtained end-to-end delay values are computed and the resultant value is illustrated in Table 3. The delay value is computed as the time taken to transmit and receive while broadcasting packets in the network.

Table 3 illustrated the end-to-end delay value of the PQDT,[14] TDSEE,[15] and LAEEBA.[16] Among the three approaches, the introduced BOATSEE approach attains the minimum delay value (77.43 s) compared to the other methods such as PQDT (133.68 s), TDSEE (111.52 s), and LAEEBA (93.45 s). The obtained results, graphical analysis is illustrated in Figure 4.

TABLE 2 Performance metrics

Parameters	Values
End to end delay	$\mathbf{Delay = QD + PD + PGD}$ **QD is the queuing delay, PD is processing delay, and PGD is the propagation delay**
Energy consumption	$\mathbf{EUF = EU/TE \times 100}$ EU is the energy utilization, TE is the transmission energy
Packet delivery rate	$\mathbf{PDR = \frac{No.\ of\ packets\ transmitted\ successfully}{No.\ of\ packets\ generated} \times 100}$
Packet loss rate	$\mathbf{PLR = \frac{No.\ of\ packets\ lossed}{No.\ of\ packets\ sent} \times 100}$

TABLE 3 End to end delay

	End to end delay			
Number of nodes	PQDT	TDSE	LAEEBA	BOATSEE
10	56.4	51.78	46.9	40.9
20	63.5	61.13	56.	52.3
40	78.8	66.2	62.8	57.39
50	112.3	98.97	83.86	67.2
70	142.9	113.2	91.47	87.4
80	163	142.5	112.4	90.4
100	195	169	128	100.4
120	257.29	189.39	167	123.47

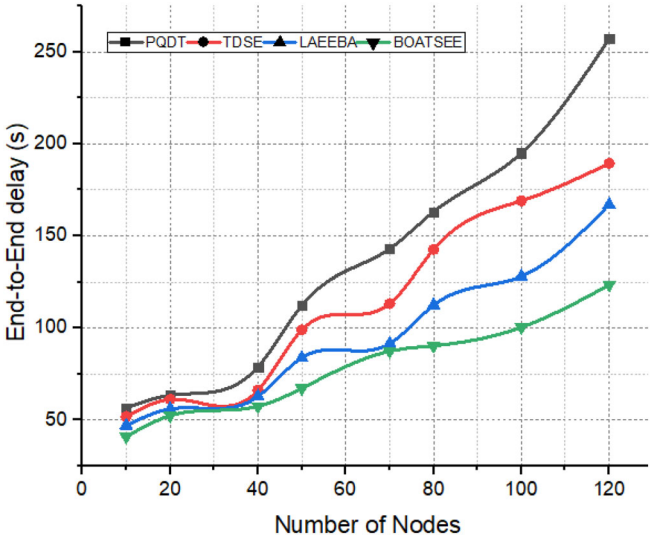


FIGURE 4 End to end delay

TABLE 4 Packet delivery ratio

	Packet delivery ratio			
Count of nodes	**PQDT**	**TDSE**	**LAEEBA**	**BOATSEE**
10	56.4	51.78	46.9	40.9
20	63.5	61.13	56.	52.3
40	78.8	66.2	62.8	57.39
50	112.3	98.97	83.86	67.2
70	142.9	113.2	91.47	87.4
80	163	142.5	112.4	90.4
100	195	169	128	100.4
120	257.29	189.39	167	123.47

The introduced method uses the cluster head (CH) that selects according to the butterfly characteristics. The selected cluster heads chosen the cluster member within the base station range. This helps to identify the cluster members according to the threshold value. The effective utilization of these cluster members is more helpful in predicting the shortest path from source to destination. Therefore, the data transmission is performed at speed and the delay has been reduced.

Further, the periodical data transmission is also performed when the critical data is entered into the broadcasting process. The minimum delay of the system directly ensures a high packet delivery rate. Then the obtained results are illustrated in Table 4.

Table 4 illustrated the packet delivery rate of the PQDT,[14] TDSEE,[15] and LAEEBA.[16] Among the three approaches, the introduced BOATSEE approach attains the maximum delivery rate (98.34%) compared to the other methods such as PQDT (88.85%), TDSEE (91.5%), and LAEEBA (93.65%). The obtained results, graphical analysis is illustrated in Figure 5.

Figure 5 illustrates the packet delivery rate analysis of the proposed BOATSEE approach compared with existing methods such as PQDT, TDSE, and LAEEBA. Measuring packet delivery ratio (PDR) can be determined by comparing the total number of packets transmitted from one network node to another and calculating the PDR as a percentage. Ideally, all of the data packets will arrive at their intended destination. The introduced approach uses the $\boldsymbol{b_u^{it+1}} = \boldsymbol{b_u^{it}} + \left(\boldsymbol{rnd^2} * \boldsymbol{h^*} - \boldsymbol{b_u^{it}}\right) * \boldsymbol{fr_u}$ local search results while selecting the cluster head. The selected CH continuously updates the attribute values, threshold values, and packet information to the members and users. The destination successfully

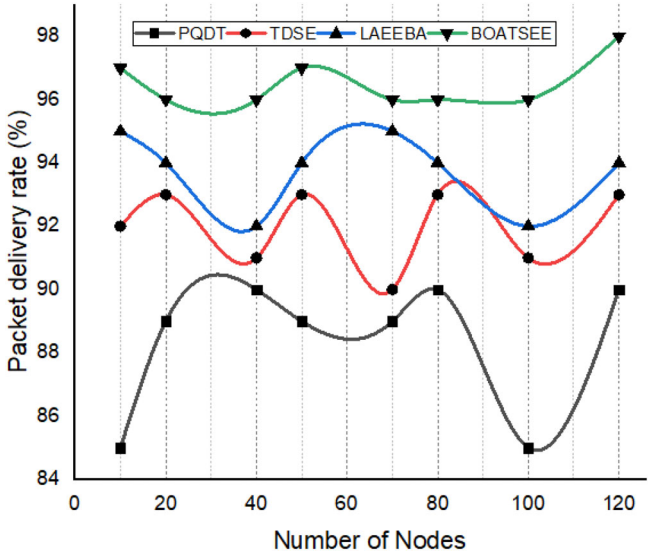


FIGURE 5 Packet delivery ratio

TABLE 5 Energy consumption factor

Count of nodes	PQDT	TDSE	LAEEBA	BOATSEE
10	3.522	4.14	2.124	1.98
20	3.834	4.745	2.345	2.03
40	4.13	5.222	2.521	2.23
50	4.845	5.656	3.156	2.98
70	5.32	6.462	3.73	3.28
80	6.25	6.911	4.167	3.86
100	7.21	8.35	5.221	4.79
120	7.98	8.97	6.146	5.23

retrieves the transferred information due to the effective identification shortest path. Although the system gives the maximum packet delivery rate, it should consume minimum energy while transmitting data. The low consumption of energy value reduces the packet loss while broadcasting. Then, the energy utilization of each node in the WBAN is computed and tabulated in Table 5.

Table 5 shows that the BOATSEE approach attains a high packet delivery ratio and consumes a low value of energy (3.29 J) contrasted to alternate methods like PQDT[14] (5.38 J), TDSEE[15] (6.30 J), and LAEEBA[16](3.67 J). The graphical analysis of the energy utilization factor is illustrated in Figure 6.

Further, the system's reliability was investigated using the packet loss rate. Figure 6 illustrates the energy utilization factor. The method utilizes the cluster head before transmitting data to the destination. The clusters are formed according to the energy and path reliability factor, which helps identify the exact data transfer path. The effective selection of paths minimizes energy consumption and packet loss. The minimum packet loss directly indicates the reliability of the system. In addition, the low energy consumption indicates that the system has a maximum network lifetime value compared to the other methods. Then the obtained packet loss rate is illustrated in Figure 7.

Based on the Figure 7, it clearly states that the BOATSEE approach attains the low packet loss ratio (0.12%) contrasted to alternate techniques like PQDT[14] (0.6%), TDSEE[15] (0.38%), and LAEEBA[16] (0.29%). Thus the introduced system broadcasts the healthcare information from sender to receiver with less loss and a high packet delivery rate.

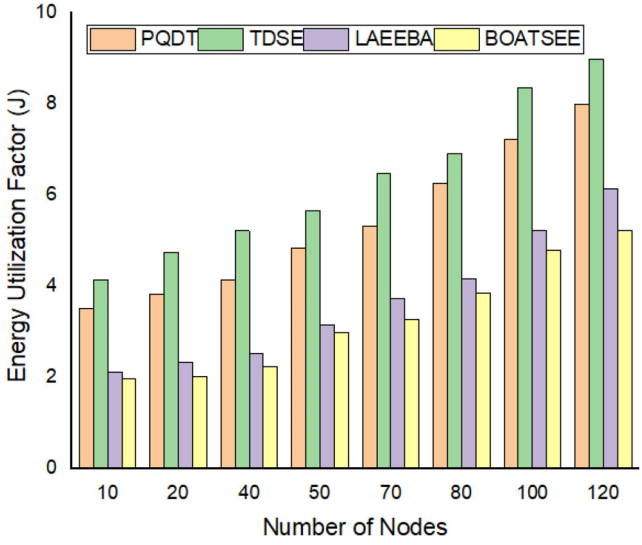


FIGURE 6 Energy utilization factor

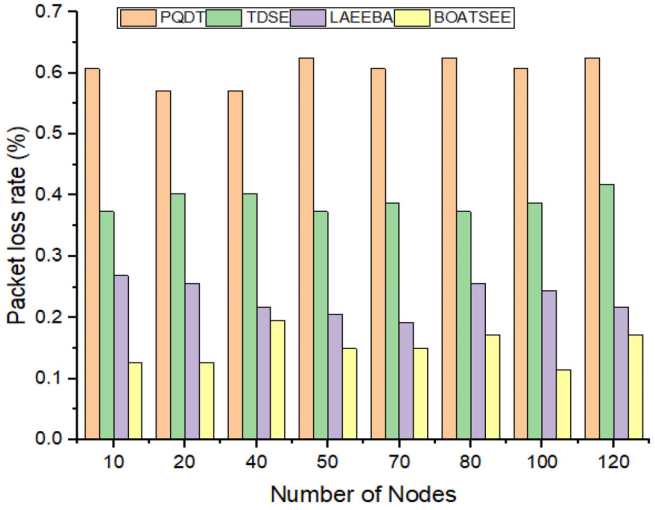


FIGURE 7 Packet loss rate

6 | CONCLUSION

Thus the article analyzed the BOATSEE routing protocol dependent health information transfer mechanism. Encrypted data is protected using the blowfish technique and the Henon-Chen chaotic dynamical systems (CDS). Over satellite and other conventional digital pictures of image processing verified the security of our suggested encryption scheme. Our suggested encryption technique is used equally at both the transmitting and receiving end of satellite communication. Telemetry data and hefty payloads are sent using standard wireless media in satellite communication. The sensed health details are transmitted by maintaining the data's reliability and quality. Here, the cluster head is chosen depending on the attributes and bacterial optimization algorithm. The cluster head is chosen during this process by investigating the path reliability and energy utilization factor. The cluster members are analyzed to predict the shortest path. The chosen path is more helpful in transmitting data with minimum time and low computation complexity. In addition, the path reliability value is estimated for every data transmission process. This computation reduces the packet loss and delays in transmitting the packet. The system's security is enhanced using the proposed encryption algorithm based on the multidimensional chaotic map. NS2 simulator with a 4 to 6-m distance hospital scenario is used to develop the proposed solution. Then the discussed system is developed using the NS2 simulator tool in which the BOATSEE approach has a 0.12% loss rate and

98.34% packet delivery rate. In the future, the system's efficiency will be improved by using the meta-heuristic routing selection process to maintain system flexibility.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

DATA AVAILABILITY STATEMENT

Research data are not shared.

REFERENCES

1. Saha R, Biswas S, Sarma S, Karmakar S, Das P. Design and implementation of routing algorithm to enhance network lifetime in WBAN. *Wirel Pers Commun*. 2021;118(2):961-998.
2. Karmakar K, Saif S, Das P, Neogy S, Biswas S. FDRF: fault detection and recovery framework for seamless data transmission in remote health monitoring using WBAN. *Wirel Pers Commun*. 2021;1-32.
3. Munivel KV, Samraj T, Kandasamy V, Chilamkurti N. Improving the lifetime of an out-patient implanted medical device using a novel flower pollination-based optimization algorithm in WBAN systems. *Mathematics*. 2020;8(12):2189.
4. Singh R, Joshi A, Mohapatra AK, Jha VN. An efficient implementation of revocable functionality in authentication protocol for wireless body area network. *J Inf Optim Sci*. 2021;42(2):321-331.
5. Barazanchi A, Israa HR, Abdulshaheed MS, Sidek B. A survey: issues and challenges of communication technologies in WBAN. *Sustain Eng Innov*. 2020;1(2):84-97.
6. Vignesh MR, Sivakumar S. Healthcare sensors issues, challenges & security threats in wireless body area network: a comprehensive survey. *IJTSRD*. 2021;5(4):989-997.
7. Singh R, Sinha S, Anand S, Sen M. Wireless body area network: an application of IoT and its issuses—a survey. *Comput Intell Pattern Recognit*. 2020;1120:285-293.
8. Memon S, Wang J, Bhangwar AR, et al. Temperature and reliability-aware routing protocol for wireless body area networks. *IEEE Access*. 2021;9:140413-140423.
9. Almuhaideb AM, Alqudaihi KS. A lightweight and secure anonymity preserving protocol for WBAN. *IEEE Access*. 2020;8:178183-178194.
10. Salem O, Alsubhi K, Mehaoua A, Boutaba R. Markov models for anomaly detection in wireless body area networks for secure health monitoring. *IEEE J Sel Areas Commun*. 2020;39(2):526-540.
11. Wang T, Fengye H, Cao F, Mao Z, Ling Z. Sum-throughput maximization based on the significance and fairness of sensors for energy and information transfer in virtual MIMO-WBAN. *IEEE Trans Veh Technol*. 2020;69(11):13400-13409.
12. Al Rasyid M Harun U, Nadhori IU et al. Anomaly detection in wireless body area network using Mahalanobis distance and sequential minimal optimization regression.Proceedings of the 2021 International Seminar on Application for Technology of Information and Communication (iSemantic); 2021:64-69; IEEE.
13. Huzooree G, Khedo KK, Joonas N. Data reliability and quality in body area networks for diabetes monitoring. In: Maheswar R, Kanagachidambaresan G, Jayaparvathy R, Thampi S, eds. *Body Area Network Challenges and Solutions*. Springer; 2019:55-86.
14. Ventura JM, Fajardo A, Medina R. Priority based data transmission for WBAN. *Int J Electr Comput Eng*. 2019;9(5):3671.
15. Goyal R, Bhadauria HS, Patel RB, Prasad D. TDMA based delay sensitive and energy efficient protocol for WBAN. *J Eng Sci Technol*. 2017;12(4):1067-1080.
16. Ullah K, Khan H. Fog-LAEEBA: fog-assisted link aware and energy efficient protocol for wireless body area network. *Acta Univ Sapientiae, Inform*. 2021;13(1):180-194.
17. Ullah F, Ullah Z, Ahmad S, Islam IU, Rehman SU, Iqbal J. Traffic priority based delay-aware and energy efficient path allocation routing protocol for wireless body area network. *J Ambient Intell Humaniz Comput*. 2019;10(10):3775-3794.
18. Kour K. An energy efficient routing algorithm for Wban. *Turk J Comput Math Educ*. 2021;12(10):7174-7180.

How to cite this article: Santhalakshmi M, Kavitha P. Medical data quality management using butterfly optimization with adaptive threshold sensitive energy-efficient routing protocol and multidimensional chaotic blowfish encryption in wireless body networks. *Trans Emerging Tel Tech*. 2022;e4619. doi: 10.1002/ett.4619