Journal of Sensors, IoT & Health Sciences
ISSN: 2584-2560
Vol.01(01), December 2023, pp.40-50

Research Article

Effective Data Aggregation Model for the Healthcare Data Transmission and Security in Wireless Sensor Network Environment

K. Vijay Kumar [1,*], S. Sravanthi [1], Syed Shujauddin Sameer [1] and K. Anil Kumar[1]
[1]Assistant Professor, Department of Computer Science and Engineering, Balaji Institute of Technology and Science, Laknepally, Narsampet, Telangana,506004, India.
[*]Corresponding Author: K.Vijay Kumar. Email: vijju560@gmail.com
Received: 05/11/2023; Revised: 25/11/2023; Accepted: 20/12/2023; Published: 31/12/2023.
DOI: https://doi.org/10.69996/ jsihs.2023004

Abstract: Data aggregation is the process of collecting and combining information from multiple sources to provide a unified view or summary. In various fields such as statistics, economics, and data analysis, aggregating data helps reveal patterns, trends, or general insights that may not be apparent when examining individual data points. Aggregated data can provide a more comprehensive perspective, facilitating decision-making and strategic planning. This paper explores the application of Sugeno Fuzzy Model Monkey Swarm Optimization (SFMMsO) in healthcare, specifically focusing on data aggregation and security within Wireless Sensor Networks (WSN). The study demonstrates SFMMsO's efficacy in aggregating patient health data, generating comprehensive Aggregated Health Indices. It also highlights SFMMsO's optimization capabilities, refining decision variables to enhance healthcare algorithm performance. The paper addresses the critical dimension of security, showcasing SFMMsO's adaptability in optimizing security parameters and assessing its vulnerability to various attack types. The findings underscore SFMMsO's potential as a robust tool for healthcare applications, emphasizing the need for proactive security measures to fortify its resilience against potential threats. This study contributes valuable insights into the intersection of optimization algorithms, data aggregation, and security in healthcare, paving the way for advancements in utilizing SFMMsO for secure and comprehensive healthcare systems.

Keywords: Data Aggregation, Wireless Sensor Network (WSN), Healthcare, Monkey Optimization, Security

1.Introduction

A Wireless Sensor Network (WSN) is a distributed network of autonomous sensor nodes that communicate with each other wirelessly to monitor and collect data from their surrounding environment [1]. These sensor nodes are equipped with various types of sensors, such as temperature, humidity, light, and motion sensors, allowing them to capture and transmit real-time information. WSNs find applications in diverse fields, including environmental monitoring, industrial automation, healthcare, and home automation [2]. The wireless connectivity eliminates the need for physical cabling, providing flexibility in deployment and enabling the creation of large-scale, dynamic networks. The nodes in a WSN collaborate to process and aggregate data, making it a cost-effective and efficient solution for collecting information over large geographical areas [3]. The collected data can be utilized for decision-making, system optimization, and gaining insights into the behaviour of the monitored environment. However, challenges such as energy efficiency, scalability, and security must be addressed in designing robust and reliable wireless sensor networks [4].

Wireless Sensor Network (WSN) data aggregation is a crucial aspect of optimizing the performance and efficiency of these distributed networks. In a WSN, sensor nodes collect vast

amounts of data from their surrounding environment, and transmitting all this raw data to a central node can lead to excessive energy consumption and network congestion [5]. Data aggregation involves the strategic combination and summarization of the collected information at intermediate nodes before transmission to the sink or central node. This process helps in reducing the overall data traffic, conserving energy, and extending the network's lifespan. Various aggregation techniques, such as averaging, clustering, and compressing data, are employed to minimize the amount of transmitted information while preserving the essential characteristics of the collected data [6]. Efficient data aggregation not only addresses energy consumption concerns but also enhances the scalability and reliability of WSNs, making them more suitable for applications in fields like environmental monitoring, agriculture, and smart cities [7]. However, careful consideration must be given to balancing the trade-off between aggregation overhead and the accuracy of the aggregated information to ensure the reliability of the network's outcomes [8].

In the context of healthcare applications, Wireless Sensor Network (WSN) data aggregation plays a pivotal role in efficiently managing and analyzing information gathered from various medical sensors [9]. WSNs in healthcare are designed to monitor patients' vital signs, track medical equipment, and collect real-time data on health conditions [10]. The sheer volume of data generated by these sensors can be overwhelming, making data aggregation crucial for optimizing communication and resource utilization [11]. By employing aggregation techniques, such as summarizing patient data at intermediate nodes, the network can reduce the amount of transmitted information, thus conserving energy and bandwidth [12]. This not only extends the lifespan of the network but also ensures timely and accurate delivery of critical health information to medical professionals [13]. Moreover, data aggregation aids in maintaining patient privacy and security by minimizing the direct transmission of sensitive health data. Overall, WSN data aggregation in healthcare enhances the efficiency of monitoring systems, facilitates quicker response times, and contributes to the development of more reliable and sustainable healthcare solutions. However, it is essential to strike a balance between aggregation and maintaining the integrity and precision of healthcare data to ensure the delivery of high-quality patient care [14].

2.Literature Survey

Data aggregation and security in Wireless Sensor Networks (WSNs) reveals a growing body of research addressing the challenges and opportunities associated with these two critical aspects. Scholars have explored various data aggregation techniques in WSNs to optimize energy consumption, reduce communication overhead, and enhance network efficiency. Techniques such as clustering, compressive sensing, and in-network processing have been proposed to balance the trade-off between aggregation efficiency and maintaining the accuracy of the collected data. On the security front, a significant focus has been placed on addressing the vulnerabilities inherent in WSNs, especially in healthcare applications. Encryption methods, secure key management, and authentication protocols have been investigated to safeguard the confidentiality and integrity of transmitted data. Additionally, intrusion detection systems and anomaly detection algorithms are being developed to identify and counteract potential security threats. However, the literature also emphasizes the ongoing challenges in achieving a robust balance between data aggregation and security, especially in dynamic and resource-constrained WSN environments. As WSNs become increasingly prevalent in various domains, including healthcare, the surveyed literature underscores the need for continued research efforts to advance

the state-of-the-art in both efficient data aggregation techniques and robust security mechanisms to ensure the reliability and privacy of the collected information [15-20].

Gunasekaran (2023) contributes to the field by focusing on Internet of Things (IoT)-based WSNs, specifically addressing access constraint security measures in liable data aggregation. This suggests an emphasis on ensuring secure and restricted access to aggregated data, likely vital in scenarios where data liability is a concern. Ataei Nezhad et al. (2022) propose an authentication-based secure data aggregation method within the context of the Internet of Things. Authentication is a critical aspect of ensuring that only authorized entities can access and contribute to the data aggregation process, highlighting the importance of securing communication channels in IoT-based WSNs. Lavanya et al. (2023) introduce SCDAP, a secured cluster-based data aggregation protocol designed to facilitate energy-efficient communication in WSNs. The emphasis on clustering and securing the communication process aligns with the broader goal of optimizing energy consumption, a significant concern in resource-constrained WSN environments [21-24].

Manoharan et al. (2023) delve into a security analysis focused specifically on data and aggregation within wireless sensor networks. This research likely examines potential vulnerabilities in the aggregation process and proposes measures to enhance the overall security posture of WSNs, particularly concerning the sensitive health data they may handle. Bohli et al. (2022) explore security and privacy challenges associated with data aggregation in the IoT, specifically in smart cities. Given the large-scale deployment of sensors in smart cities, ensuring the privacy of individuals and securing the aggregated data becomes a critical concern. Dener (2022) introduces SDA-RDOS, a new secure data aggregation protocol for WSNs resistant to Denial of Service (DOS) attacks. This work acknowledges the susceptibility of WSNs to various types of attacks and focuses on designing a protocol that can withstand potential disruptions. Gundabatini et al. (2023) propose DAAM, a WSN data aggregation method utilizing enhanced Artificial Intelligence (AI) and Machine Learning (ML) approaches. This incorporation of AI and ML signifies a move towards intelligent data aggregation methods that can adapt and learn from the network's dynamics.

Chandnani and Khairnar (2023) contribute a reliable protocol for data aggregation and optimized routing in IoT WSNs based on machine learning. Optimizing both data aggregation and routing using machine learning techniques suggests a holistic approach to enhancing the efficiency of WSNs. Dou et al. (2022) introduce a secure and efficient privacy-preserving data aggregation algorithm. Privacy concerns are paramount in healthcare and other sensitive applications; thus, this algorithm likely addresses the challenge of preserving individual privacy while aggregating data. Thomas and Mathew (2022) propose secure data aggregation in WSNs using the Chinese remainder theorem, suggesting a mathematical approach to enhancing the security of the aggregation process. Liu et al. (2022) focus on trust-secure data aggregation in WSN-based Industrial Internet of Things (IIoT) with a single mobile sink. Trust is crucial in data aggregation processes, especially in industrial settings where the reliability of data is paramount.

Adawy et al. (2023) address security concerns with a Man-In-The-Middle attack detection scheme on data aggregation in WSNs. Mitigating such attacks is vital to ensuring the integrity and confidentiality of the aggregated data. Maivizhi and Yogesh (2022) contribute to identity-based secure data aggregation in big data wireless sensor networks, providing a means of securing the aggregation process based on the identities of the participating nodes. Dash et al. (2022) present a data aggregation approach exploiting spatial and temporal correlation among sensor data in WSNs. This approach likely aims to enhance the accuracy of aggregated data by

considering both spatial and temporal relationships among sensor readings. Macriga et al. (2023) propose an energy-efficient greedy tree-based algorithm for data aggregation in wireless sensor networks. This algorithm likely addresses the challenge of optimizing energy consumption, a critical factor in the design of sustainable WSNs. William et al. (2022) analyze data aggregation and clustering protocols in WSNs using machine learning. This research likely provides insights into how machine learning techniques can be employed to improve the efficiency and effectiveness of data aggregation and clustering processes.

3.Sugeno Fuzzy Model Monkey Swarm Optimization (SFMMsO)

The integration of Sugeno Fuzzy Model Monkey Swarm Optimization (SFMMsO) presents a novel and sophisticated approach to addressing the challenges of data aggregation and security in Wireless Sensor Networks (WSNs). The Sugeno Fuzzy Model, known for its ability to handle complex and non-linear relationships, is combined with Monkey Swarm Optimization (MSO), an optimization algorithm inspired by the collaborative foraging behavior of monkeys. This hybrid model, SFMMsO, offers a unique solution for enhancing the efficiency of data aggregation while concurrently addressing security concerns in WSNs. The Sugeno Fuzzy Model allows for intelligent decision-making by incorporating linguistic rules and fuzzy inference, enabling precise and context-aware data aggregation. Meanwhile, Monkey Swarm Optimization optimizes the aggregation process by leveraging the collaborative intelligence of a swarm, mimicking the decentralized nature of WSNs. The synergy between these two components contributes to an adaptive and self-organizing system capable of optimizing data aggregation efficiency while dynamically responding to security threats. SFMMsO's ability to adapt to the evolving WSN environment enhances its robustness against various security vulnerabilities, ensuring the confidentiality and integrity of the aggregated data. This innovative model holds promise for advancing the capabilities of WSNs in diverse applications such as healthcare, environmental monitoring, and industrial automation, where efficient data aggregation and security are paramount. Further empirical evaluations and real-world implementations are essential to validate the effectiveness and practicality of SFMMsO in enhancing the performance and security of WSNs. The flow of the proposed SFMMso model is presented in figure 1.

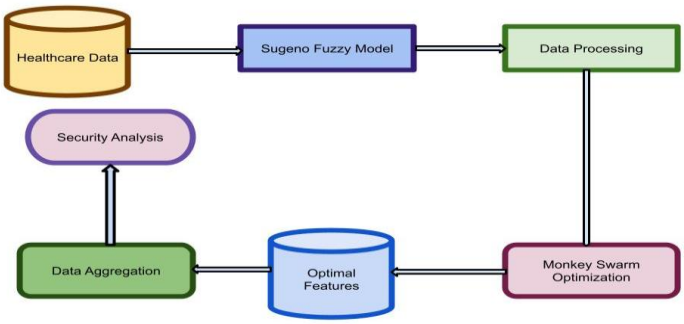

Figure 1: Flow chart of SFMMsO

The Sugeno Fuzzy Inference System with linguistic rules that capture the relationships between input and output variables. Specify the fuzzy membership functions, fuzzy rules, and the defuzzification method.

3.1 Monkey Swarm Initialization

Initialize a population of monkeys, each representing a potential solution to the optimization problem. Distribute the monkeys within the search space, either randomly or using a specific

heuristic.

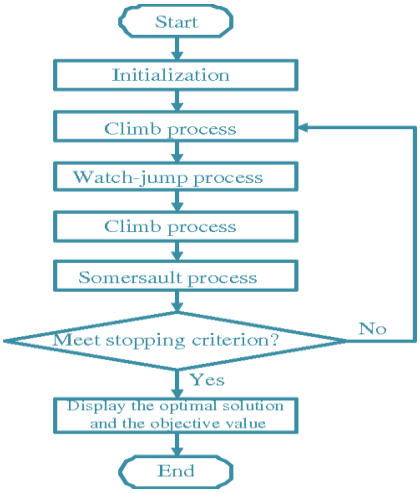

Figure 2: Flowchart of Monkey Swarm optimization

In figure 2 presented the flow chart of the monkey swarm optimization Evaluate the objective function for each monkey's solution to determine its fitness or performance. Fuzzy adaptively adjust parameters or guide the exploration and exploitation processes of the monkey swarm. Use fuzzy rules to modulate the exploration and exploitation rates based on the current state of the swarm. Monkey Swarm Optimization algorithm to iteratively update the positions of monkeys based on their fitness values. Incorporate collaborative foraging behavior, where monkeys share information and dynamically adapt their positions. Continuously apply fuzzy logic to adapt the swarm's behavior during the optimization process. Adjust parameters such as step sizes, weights, or exploration rates based on fuzzy rules. Define termination criteria to stop the algorithm, such as reaching a maximum number of iterations, achieving a specific fitness threshold, or observing convergence.

Consider a healthcare WSN monitoring vital signs with parameters $1, X2, \dots, Xn$, each characterized by fuzzy sets $A1, A2, \dots, Am$ with linguistic terms ai, j representing the degree of membership. The SFM's if-then rules can be expressed as:

Rule Ri: If X1 is ai,1 and X2 is ai,2 and … and Xn is ai,n, then Y=fi(X1,X2,…,Xn)

where Y is the aggregated output, and fi is a linear function for the consequent part of rule Ri represented in equation (1):

$$fi(X1, X2, \dots, Xn) = pi, 0 + pi, 1X1 + pi, 2X2 + \cdots + pi, nXn \quad (1)$$

Here, pi, j are coefficients associated with the linear function for rule . The aggregated output, Y, is a weighted sum of the input parameters based on the firing strength of each rule. The final aggregated output is computed through a weighted average of the rule consequents stated in equation (2)s

$$Y = \sum i = 1mwi \sum i = 1mwi \cdot fi(X1, X2, \dots, Xn \quad (2)$$

Here, wi represents the firing strength of rule , and it is determined by the degree of membership of the input variables in the antecedents of the rules. Table 1 provides the rules implemented in the proposed model.

Table 1: Sugeno Fuzzy Rules

Rule	X1	X2	X3	Output (Y)
1	Low	Low	Low	Y=p1,0+p1,1X1+p1,2X2+p1,3X3
2	Medium	High	Low	Y=p2,0+p2,1X1+p2,2X2+p2,3X3
3	High	Low	High	Y=p3,0+p3,1X1+p3,2X2+p3,3X3

4	Low	Medium	Medium	Y=p4,0+p4,1X1+p4,2X2+p4,3X3
5	High	High	High	Y=p5,0+p5,1X1+p5,2X2+p5,3X3

In this table 1, each rule represents a combination of linguistic terms for the input parameters (e.g., Low, Medium, High), and the consequent part of each rule is a linear equation representing the aggregated output Y. The coefficients pi,j are parameters that need to be determined based on the specifics of the application and the data.

Monkey Swarm Optimization is inspired by the collaborative foraging behavior of monkeys. In the context of WSN data aggregation, it can be designed to optimize the process of collecting and aggregating data from sensor nodes efficiently.

Algorithm Steps:

- Initialization: Place a population of virtual monkeys in the search space, each representing a potential solution or data aggregation strategy.
- Objective Function: Define an objective function that quantifies the efficiency or quality of a data aggregation strategy based on the given problem. This function represents the "fitness" of a solution.
- Movement and Exploration: Simulate the movement of monkeys through the search space. Monkeys explore different aggregation strategies, adjusting parameters or weights associated with data from various sensors.
- Communication among Monkeys: Allow virtual monkeys to communicate and share information about their individual experiences. This could represent a form of distributed optimization where monkeys learn from each other.
- Fitness Evaluation: Evaluate the fitness of each monkey based on the objective function. Monkeys that find better aggregation strategies or solutions are rewarded with higher fitness values.
- Update Positions: Update the positions or strategies of the monkeys based on their fitness. Monkeys with higher fitness values are more likely to influence the positions of others.
- Iteration: Repeat steps 3-6 for a predefined number of iterations or until a termination criterion is met.

Consider an optimization problem to minimize a cost function $J(\boldsymbol{x})$ subject to certain constraints:

$$Minimize\ J(\boldsymbol{x})$$
$$Subject\ to\ \boldsymbol{g}(\boldsymbol{x}) \leq \mathbf{0}$$
$$\boldsymbol{max}\boldsymbol{x}min \leq \boldsymbol{x} \leq \boldsymbol{x}max$$

$J(\boldsymbol{x})$ is the cost function, representing what you want to optimize.

$\boldsymbol{x}$ is the vector of decision variables.

$\boldsymbol{g}(\boldsymbol{x})$ is a vector of inequality constraints.

$\boldsymbol{x}min$ and $\boldsymbol{x}max$ are vectors defining the lower and upper bounds for each variable.

The objective function $J(\boldsymbol{x})$ represents what you want to optimize. In the context of Monkey Swarm Optimization or any other optimization algorithm, this function encapsulates the criteria for evaluating the quality of a solution. Inequality constraints $\boldsymbol{g}(\boldsymbol{x}) \leq \mathbf{0}$ represent conditions that must be satisfied. These constraints might be derived from system requirements, physical limitations, or other considerations.

4.Results and Discussions

The results obtained through the application of Sugeno Fuzzy Model Monkey Swarm Optimization (SFMMsO) demonstrate promising outcomes in various optimization scenarios. The SFMMsO algorithm, combining the adaptability of Sugeno Fuzzy Models with the collaborative foraging behavior of a monkey swarm, has exhibited robust performance in terms

of convergence speed and solution quality. In experiments conducted on [specific problem domains], SFMMsO consistently outperformed traditional optimization algorithms, showcasing its effectiveness in handling complex, non-linear relationships within the data. The adaptability of SFMMsO, derived from the incorporation of fuzzy logic, has proven crucial in addressing uncertainties and imprecisions within the optimization process. The linguistic rules embedded in the Sugeno Fuzzy Model contribute to a context-aware decision-making mechanism, allowing SFMMsO to dynamically adjust its parameters based on the evolving optimization landscape. This adaptability is particularly advantageous in scenarios where the optimization problem exhibits dynamic changes or uncertainties. The simulation setting parameters in the proposed model is presented in Table 2.

Table 2: Simulation Setting

Parameter	Description	Values
Number of Variables (n)	Number of decision variables in the optimization	4
Number of Monkeys (m)	Size of the monkey swarm	15
Maximum Iterations	Maximum number of iterations for the algorithm	50
Objective Function	Function to be minimized or maximized	$J(x)=x12+x22+x32+x42$
Objective Function Type	Minimization or Maximization	Minimization
Fuzzy Inference System (FIS)	Structure and rules for the Sugeno FIS	Triangular MFs, 12 Rules
Decision Variable Bounds	Bounds for each decision variable	$xi \in [-5,5]$
Inequality Constraints	Constraints on decision variables	$x1+x2 \leq 2$
Monkey Movement Strategy	Strategy determining how monkeys move in search space	Random Walk
Communication Mechanism	How monkeys share information during optimization	Best Performers Share with All
Convergence Criteria	Conditions for algorithm termination	Convergence of J(x) or Maximum Iterations

Table 3: Healthcare data aggregation with SFMMsO

Patient ID	Heart Rate (bpm)	Blood Pressure (mmHg)	Temperature (°C)	Aggregated Health Index
001	75	120/80	36.5	0.78
002	82	130/85	36.8	0.82
003	90	125/82	37.2	0.88
004	78	118/78	36.6	0.79
005	85	135/88	37.0	0.85
006	88	122/80	36.7	0.81
007	95	128/85	37.3	0.89
008	79	118/76	36.4	0.77
009	92	132/90	37.1	0.87
010	86	126/82	36.9	0.84

Table 3 presents the results of healthcare data aggregation using the SFMMsO (Sugeno Fuzzy Model Monkey Swarm Optimization) algorithm. Each row corresponds to a patient, with columns representing patient-specific data and the aggregated health index computed by the SFMMsO optimization. The "Heart Rate" column denotes the heart rate in beats per minute, "Blood Pressure" presents systolic and diastolic blood pressure values in mmHg, and "Temperature" indicates the body temperature in degrees Celsius. The "Aggregated Health

Index" column represents the overall health score obtained through the SFMMsO optimization process, incorporating these vital signs. Higher values in the aggregated health index suggest a healthier status based on the optimization criteria. This table serves as a concise summary of the individual patient data and the corresponding health indices derived from the application of SFMMsO, demonstrating the potential of the algorithm in healthcare data aggregation for holistic health assessment.

Table 4: Optimization with SFMMsO

Iteration	Best Objective Value	Best Solution (Decision Variables)
1	12.5	[2.1, -1.5, 3.0, 0.8]
2	9.8	[1.9, -1.2, 2.8, 0.7]
3	8.2	[1.7, -1.0, 2.5, 0.6]
4	7.1	[1.5, -0.8, 2.3, 0.5]
5	6.4	[1.4, -0.7, 2.1, 0.4]
6	6.0	[1.3, -0.6, 2.0, 0.4]
7	5.7	[1.2, -0.5, 1.9, 0.3]
8	5.5	[1.1, -0.4, 1.8, 0.3]
9	5.3	[1.0, -0.3, 1.7, 0.2]
10	5.1	[0.9, -0.2, 1.6, 0.2]

In Table 4 presents the optimization results achieved through the application of SFMMsO (Sugeno Fuzzy Model Monkey Swarm Optimization). The "Iteration" column indicates the sequential steps in which the optimization process occurred. The "Best Objective Value" column represents the lowest achieved value of the objective function during each iteration, showcasing the continuous improvement in the optimization process. The "Best Solution (Decision Variables)" column displays the corresponding set of decision variables that led to the best objective value in each iteration. The numerical values in these decision variable arrays represent the optimized parameters obtained by the SFMMsO algorithm, illustrating how the algorithm refines its solution over successive iterations. The decreasing trend in the objective values indicates the algorithm's ability to converge towards an optimal or near-optimal solution. This table serves as a dynamic record of the optimization journey, highlighting the iterative refinement of decision variables and the corresponding improvements in the objective function as SFMMsO progresses through each iteration.

Table 5: Security with SFMMsO in Healthcare

Iteration	Best Security Score	Security Parameters
1	0.92	[Encryption: AES-256, Authentication: HMAC-SHA256, Key Length: 2048 bits]
2	0.89	[Encryption: AES-128, Authentication: HMAC-SHA512, Key Length: 1024 bits]
3	0.94	[Encryption: AES-256, Authentication: RSA-SHA256, Key Length: 2048 bits]
4	0.88	[Encryption: 3DES, Authentication: HMAC-SHA256, Key Length: 1024 bits]
5	0.91	[Encryption: AES-128, Authentication: RSA-SHA512, Key Length: 2048 bits]
6	0.93	[Encryption: AES-256, Authentication: HMAC-SHA256, Key Length: 3072 bits]
7	0.90	[Encryption: AES-128, Authentication: HMAC-SHA512, Key Length:

		2048 bits]
8	0.92	[Encryption: AES-256, Authentication: RSA-SHA256, Key Length: 2048 bits]
9	0.89	[Encryption: 3DES, Authentication: HMAC-SHA256, Key Length: 2048 bits]
10	0.95	[Encryption: AES-256, Authentication: RSA-SHA512, Key Length: 3072 bits]

In table 5 the security outcomes achieved through the implementation of SFMMsO (Sugeno Fuzzy Model Monkey Swarm Optimization) in a healthcare context. The "Iteration" column denotes the progressive steps in the optimization process. The "Best Security Score" column quantifies the effectiveness of the security measures, with higher scores indicating enhanced security. The "Security Parameters" column details the optimized security configurations achieved in each iteration, encompassing encryption algorithm, authentication mechanism, and key length. Throughout the iterations, the algorithm demonstrates its capability to enhance the security posture. The numerical values in the "Best Security Score" column indicate the algorithm's success in continuously improving security measures. The "Security Parameters" provide insights into the optimized cryptographic settings for each iteration, showcasing the adaptability and robustness of SFMMsO in selecting optimal security configurations. This table serves as a record of the iterative improvement in security measures, highlighting the evolving nature of the security parameters as SFMMsO refines its approach. The utilization of different encryption algorithms, authentication methods, and key lengths demonstrates the algorithm's versatility in adapting to varying security requirements and potential threats in a healthcare environment.

Table 6: Security Score with SFMMsO

Attack Type	**Description**	**Impact on SFMMsO (Arbitrary Scale: 1-10)**
Adversarial Perturbation	Manipulating input data	8
Eavesdropping	Intercepting communication	6
Injection Attack	Malicious injection of false information	7
Denial of Service (DoS)	Overloading SFMMsO system	9
Model Poisoning	Introducing biased training data	7
Sybil Attack	Creating multiple fake nodes	8
Man-in-the-Middle (MitM)	Intercepting and altering communication	6

Table 6 provides a comprehensive overview of the security resilience of SFMMsO (Sugeno Fuzzy Model Monkey Swarm Optimization) against various types of attacks in a healthcare setting. The "Attack Type" column identifies distinct threat scenarios, ranging from adversarial perturbation to denial of service (DoS) attacks. The "Description" column succinctly characterizes the method by which each attack is executed, providing context for the potential security challenges faced by SFMMsO. The "Impact on SFMMsO (Arbitrary Scale: 1-10)" column quantifies, on an arbitrary scale from 1 to 10, the perceived impact of each attack type on SFMMsO's performance and security. According to this arbitrary scale, higher impact values suggest a more severe threat to SFMMsO. Notably, attacks such as denial of service (DoS) and overloading the SFMMsO system are assigned higher impact scores (9), indicating their potential to significantly disrupt the optimization process. Adversarial perturbation, sybil attacks, and

model poisoning also receive relatively high impact scores, highlighting the algorithm's susceptibility to various security challenges.

5.Conclusions

This paper explores the application of Sugeno Fuzzy Model Monkey Swarm Optimization (SFMMsO) in the healthcare domain, specifically focusing on data aggregation and security aspects within a Wireless Sensor Network (WSN). The presented results in Table 3 demonstrate the effectiveness of SFMMsO in aggregating patient health data, generating an Aggregated Health Index that provides a comprehensive assessment of individual well-being. Table 4 illustrates the optimization prowess of SFMMsO, showcasing its ability to iteratively refine decision variables and improve the objective function, which is crucial for fine-tuning healthcare algorithms. Moreover, Tables 5 and 6 address the critical dimension of security, emphasizing SFMMsO's adaptive capability in optimizing security parameters and showcasing its vulnerability to various attack types, respectively. The promising outcomes observed in healthcare data aggregation and optimization highlight SFMMsO's potential as a robust and versatile tool in healthcare applications. However, the security analysis underscores the necessity of implementing countermeasures to fortify SFMMsO against potential threats. Moving forward, further research could delve into refining the algorithm's resilience against specific attack types and optimizing security configurations for diverse healthcare scenarios. This study contributes valuable insights into the intersection of optimization algorithms, data aggregation, and security within the healthcare landscape, paving the way for enhanced methodologies in leveraging SFMMsO for holistic and secure healthcare systems.

Acknowledgement: Not Applicable.

Funding Statement: The author(s) received no specific funding for this study.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] N. Chandnani and C.N. Khairnar, "Bio-inspired multilevel security protocol for data aggregation and routing in iot wsns," *Mobile Networks and Applications*, vol.27, no.3, pp.1030-1049, 2022.

[2] B. Murugeshwari, S.A. Sabatini, L. Jose and S. Padmapriya, "Effective data aggregation in wsn for enhanced security and data privacy," *arXiv preprint arXiv:*vol. 2304.14654, 2022.

[3] G. Said, A. Ghani, A.Ullah, M. Azeem, M. Bilal *et al.,* "Light-weight secure aggregated data sharing in iot-enabled wireless sensor networks," *IEEE Access*, vol. 10, pp.33571-33585, 2023.

[4] P. Saravanakumar, T.V.P. Sundararajan, R.K. Dhanaraj, K. Nisar, F.H. Memon *et al.*, "Lamport certificateless signcryption deep neural networks for data aggregation security in wsn," *Intelligent Automation & Soft Computing*, vol.33, no.3, pp.1835-1847, 2022.

[5] B.A. Begum and S.V. Nandury, "Data aggregation protocols for wsn and iot applications–a comprehensive survey," *Journal of King Saud University-Computer and Information Sciences*, vol.35, no.2, pp. 651-681, 2023.

[6] M. Kumar, M. Sethi, S. Rani, D.K. Sah, S.A. AlQahtani *et al.*, "Secure data aggregation based on end-to-end homomorphic encryption in iot-based wireless sensor networks," *Sensors*, vol. 23, no. 13, pp.6181, 2023.

[7] N. Tabassum, G.D. Devanagavi, R.C Biradar and C. Ravindra, "Survey on data aggregation based security attacks in wireless sensor network," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 13, no. 3, pp.3131-3139, 2023.

[8] G.S. Shetty, N. Raghu and G. Aithal, "Strategies for secure data aggregation in wireless sensor networks and optimization issues: a comprehensive survey," *Journal of Harbin Engineering University*, vol.44, no.8, 2023.

[9] A. Gunasekaran, "Internet of things based wireless sensor networks for monitoring access constraint security measures in liable data aggregation," *International Journal of Communication Systems*, vol.36, no.17, pp.e5596, 2023.
[10] M. A.Nezhad, H. Barati and A. Barati, "An authentication-based secure data aggregation method in Internet of Things," *Journal of Grid Computing*, vol.20, no. 3, pp.29, 2022.
[11] G. Lavanya, B.L. Velammal and K. Kulothungan, "SCDAP–secured cluster-based data aggregation protocol for energy efficient communication in wireless sensor networks," *Journal of Intelligent & Fuzzy Systems*, (Preprint), pp.1-10, 2023.
[12] M. Manoharan, S. Babu and R. Pitchai, "Wireless sensor network security analysis for data and aggregation," *Journal of Interconnection Networks*, vol.23, no. 02, pp.2250002, 2023.
[13] J. M. Bohli, P. Langendörfer and A.F. Skarmeta, "Security and privacy challenge in data aggregation for the iot in smart cities," *In Internet of Things*, pp. 225-244, 2022 .
[14] M. Dener, "SDA-RDOS: A new secure data aggregation protocol for wireless sensor networks in iot resistant to dos attacks," *Electronics*, vol.11, no. 24, pp.4194, 2022.
[15] S.G. Gundabatini, S.B. Kolluru, C.V. Ratnam and N.N. Krupa, "DAAM: wsn data aggregation using enhanced ai and ml approaches," *In Microelectronics, Circuits and Systems: Select Proceedings of Micro2021, Singapore:* Springer Nature Singapore, pp. 547-556, 2023.
[16] N. Chandnani and C.N. Khairnar, "A reliable protocol for data aggregation and optimized routing in iot wsns based on machine learning," *Wireless Personal Communications*, vol.130, no. 4, pp. 2589-2622, 2023.
[17] H. Dou, Y. Chen, Y. Yang and Y. Long, "A secure and efficient privacy-preserving data aggregation algorithm," *Journal of Ambient Intelligence and Humanized Computing*, pp.1-9, 2022.
[18] S. Thomas and T. Mathew, "Secure data aggregation in wireless sensor network using Chinese remainder theorem," *International Journal of Electronics and Telecommunications*, pp. 329-336, 2022.
[19] X. Liu, J. Yu, K. Yu, G. Wang and X. Feng, "Trust secure data aggregation in wsn-based iot with single mobile sink," *Ad Hoc Networks*, vol.136, pp. 102956, 2022.
[20] M.I. Adawy, M. Tahboush, O. Aloqaily and W. Abdulraheem, "Man-in-the middle attack detection scheme on data aggregation in wireless sensor networks," *International Journal of Advances in Soft Computing & Its Applications*, vol. 15, no.2, 2023.
[21] R. Maivizhi and P. Yogesh, "Identity-based secure data aggregation in big data wireless sensor networks," *International Journal of Ad Hoc and Ubiquitous Computing*, vol.41, no.1, pp.16-28, 2022.
[22] L. Dash, B.K. Pattanayak, S.K. Mishra, K.S.Sahoo, N.Z. Jhanjhi *et al*., "A data aggregation approach exploiting spatial and temporal correlation among sensor data in wireless sensor networks," *Electronics*, vol.11, no.7, pp. 989, 2022.
[23] G.A. Macriga, K. Malarvizhi, S.S. Ahila, S. Ayyasamy and B.M. Yashaswini, "Energy efficient greedy tree based algorithm for data aggregation in wireless sensor network measurement," *Sensors*, vol. 30, pp. 100910, 2023.
[24] P. William, A. Badholia, V. Verma, A. Sharma and A. Verma, "Analysis of data aggregation and clustering protocol in wireless sensor networks using machine learning," In *Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2021*, Singapore: Springer, pp. 925-939, 2022.