ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20241130002159
Original scientific paper

Integration of Improved Whale Optimization Algorithm and Deep Learning for Trust Management in Social IoT Environment

Kavitha RAVICHANDRAN*, Murugesan GURUSAMY, Ghadah ALDEHIM, Mashael MAASHI

Abstract: The Social Internet of Things (SIoT) integrates IoT with social networks, enabling autonomous device interactions and seamless data sharing. A key challenge in SIoT is ensuring secure and reliable interactions through an effective Trust Management System (TMS). This paper proposes the Integration of Improved Whale Optimization Algorithm and Deep Learning for Trust Management System (IIWOADL-TMS) to enhance trust evaluation and authentication in SIoT environments. The model computes direct and indirect trust values to assess device credibility, restricting access to untrusted nodes. It employs Long Short-Term Memory (LSTM) networks for traffic classification and dynamically determines the Threshold Trust Value (THVL) to enhance security. The Improved Whale Optimization Algorithm (IWOA) optimizes LSTM's hyperparameters, improving classification accuracy and trust assessment efficiency. Experimental evaluations demonstrate that IIWOADL-TMS outperforms existing models in trust evaluation, authentication, and secure data communication. The proposed system enhances reliability, scalability, and resilience in SIoT networks by mitigating security risks and improving trust computation mechanisms. These results highlight IIWOADL-TMS as a robust solution for secure and efficient interactions in SIoT.

Keywords: improved whale optimization algorithm (IWOA); long short-term memory (LSTM); secure data communication; social IoT (SIoT); trust management system (TMS)

1 INTRODUCTION

IoT, or "Internet of Things", denotes a network of interconnected physical entities utilising software, sensors, and various technical innovations. This network enabled devices to collect and share data, facilitating uninterrupted communication and coordination among them [1]. Consequently, physical objects become significantly more dynamic and data-oriented. Conversely, the IoT streamlines the development of platforms that interconnect diverse electronic gadgets. The SIoT enhances connection by fortifying social relationships and interactions among objects. These interactions resemble those that transpire among individuals inside social networks [2]. Devices inside this system have the capability to form social relationships, facilitating the IoT to transmit data according to established standards. This facilitates the interchange of data, trust, and scalability.

The identification of the IoT enables alterations in various facets of life, including proximity-based interactions, connections among social items, and collective ownership. As stated in [4], this leads to the creation of a dynamic environment in which devices interact and collaborate. The concept of the IoT offers a dependable approach for addressing the current challenges. The SIoT, which integrates social networks with intelligent devices, has facilitated the expansion of the IoT as a technological innovation. Thus, each entity can autonomously delineate its social connections with another entity, in accordance with the regulations set forth by the proprietors of the respective objects [5]. Items classified within this category may encompass social objects, ownership objects, co-working items, parenting objects, and co-location-related products [6]. This category may also encompass co-location items, which represent alternative sorts of relationships that can be classified collectively.

Trust is essential for the development and maintenance of social interactions. This arises from the notion that social entities can solely engage in relationships, and the participants in the connection are seen sufficiently trustworthy to mitigate the inherent risks associated with decision-making [7]. Establishing dependable connections among objects facilitates their prompt response to service demands from acknowledged entities within the system, hence diminishing the probability of malevolent objects exploiting the system [8]. Numerous academic disciplines, including sociology, psychology, and computer science, have investigated the topic of trust. The concept of trust varies across different disciplines, resulting in the absence of a globally agreed definition of trust [9]. Therefore, it is imperative to evaluate trust from the standpoint of the Internet of Things. ten Trust in the context of the IoT is defined as the assurance of achieving one's objectives within a specific environment and timeframe.

2 RELATED WORKS

Abdelghani et al. [11] present a DSL-STM solution, which is an innovative multi-level trust methodology that is both scalable and dynamic. This methodology was specifically devised for SIoT environments. Subsequently, multidimensional measures were proposed to delineate the behaviours of SIoT systems. The second method was utilised alongside a machine learning-based strategy, enabling the classification of individuals, recognition of various attack kinds, and appropriate responses. In the future, it may be feasible to propose a hybrid propagation strategy to disseminate trust values inside the system. Magdich et al. [12] give a comprehensive research study on the efficacy of trust attacks. This study aims to precisely detect node behaviours to ensure network connections are secure. Consequently, our trust evaluation technique incorporates a node behaviour analysis grounded in machine learning methodologies. Bangui et al. [13] illuminated the social dimensions of trust management within the Internet of Things, hence advancing its development. The author examines recent research encompassing various applications of the IoT across diverse environments to achieve this objective. The aim of this research is to explore how trust management might facilitate the communalisation of smart technologies across many domains. A distinct subset of the IoT is the Internet of Medical Things (IoMT), which is garnering increasing

attention from researchers and necessitates reliable connectivity among all devices.

Magdich et al. [14] provide an extensive investigation of context trust insights utilising the established TM approach referred to as "CTM-SIoT". This research aims to accurately detect hostile nodes within the SIoT to ensure secure connections across the network. During the trust assessment procedure, methodologies from machine learning were employed to evaluate the node's behaviour. The author aims to minimise interactions with service providers who exhibit aggression and insufficient abilities. Latif [15] introduces a context-sensitive trust management system known as ConTrust. This methodology is employed in the domain of the IoT. This process is employed for the selection and assignment of jobs. The application of the feature-property matching method, along with the integration of ability, satisfaction, and commitment, has enhanced the efficiency of trust evaluation and sustained context-dependent concerns. Roy et al. [16] introduced autonomous decentralised trust management systems aimed at selecting a reliable device for transactions requiring specific services. A system that employs SIoT is presented below. The developed approach utilises social interactions to assess the trust levels between connected devices, calculate the trustworthiness of unidentified devices, continuously update perceived trust values, and isolate malicious nodes within the system. Ongoing enhancements have been implemented to the trust values assessed inside the network to facilitate the utilisation of information by another device in the future. Zhang et al. [17] propose an inherent social relationship-based trust management (IRTM) technique to guarantee reliable service delivery in the IoT.

Existing studies lack an integrated framework combining deep learning-based behavioral analysis, dynamic threshold determination, and optimization techniques for trust computation. Addressing these gaps, our proposed IIWOADL-TMS enhances trust assessment accuracy and security in SIoT by leveraging LSTM for classification and IWOA for hyperparameter optimization, ensuring robust, adaptive trust management.

3 PROPOSED WORK

This research introduces a technology called IIWOADL-TMS within the SIoT Network. The IIWOADL-TMS system aims to enhance application performance and implement a secure data transmission technique, calculating both indirect and direct trust levels based on several assessment characteristics. Fig. 1 presents an illustration of the IIWOADL-TMS method workflow.

3.1 Trust Evaluation Model

A trust evaluation model was conceptualised through the application of the IIWOADL-TMS technique. Let G (V, E) be the communication inside the graph, where N signifies the number of devices represented as a set of devices = {v_1, v_2, ..., v_n}. Capillary communications, encompassing Bluetooth, Wi-Fi, ZigBee, and 5G, have been facilitated by all devices [18].

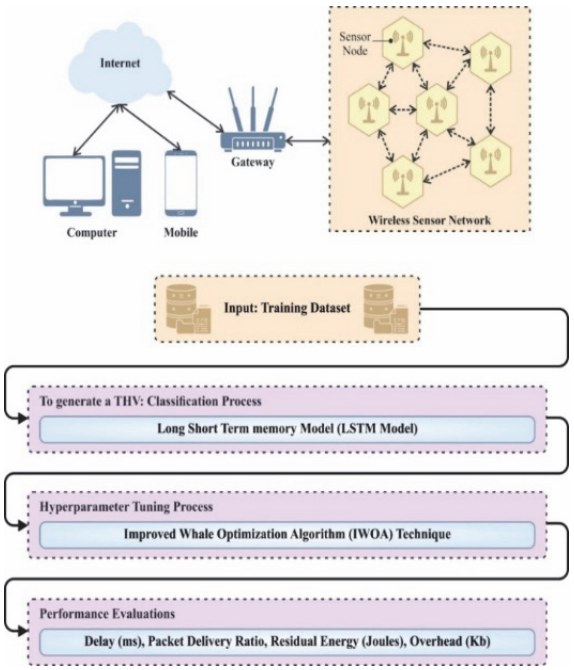

Figure 1 Proposed flow diagram

The communication channels within the devices were denoted by a set of edges represented as $E = \{e_1, e_2, \ldots, e_m\}$. The reliability of the item not associated with trustworthy SIoT has been assessed using one of three methodologies: 1) indirect trust, 2) recommended trust, or 3) direct trust. A thorough trust assessment consists of three separate components: the intrinsic trust value of the item (α), the trust value directly provided by another entity (β), and the trust value obtained through recommendations (γ).

$$\text{Overall\_Trust (OT)} = w_1\alpha + w_2\beta + w_3 r \tag{1}$$

The IIWOADL-TMS technique facilitated the design of a trust evaluation model. The communication in the graph is represented by the symbol G (V, E), where N signifies the number of devices depicted as a set of devices. The collection of devices corresponds to the values v_1, v_2, ..., v_n from the set of devices. All devices have been authorised for capillary communications, including Bluetooth, Wi-Fi, ZigBee, and 5G communications [18]. Capillary communications encompass 5G communications as well. A set of edges, represented as $E = \{e_1, e_2, \ldots, e_m\}$, was utilised to depict the communication routes existing within the devices. Indirect trust, suggested trust, and direct trust are the three approaches employed to evaluate the reliability of the non-trustworthy communication portion of the IoT. The comprehensive trust evaluation consists of three primary elements. The modules encompass the intrinsic trust value of the item (α), the trust value directly provided by another entity (β), and the trust value obtained through suggestion (γ).

$$w_1 + w_2 + w_3 = 1 \tag{2}$$

The trust value weight of the connected device is represented by w_1 and is contingent upon the preceding transaction (r^+, r^-). Conversely, r^+ and r^- denote affirmative and negative responses, respectively. These

assertions denote the aggregate quantity of services ($T_{services}$) that engaged in the delivered effective services. The weight w_1 can be expressed in Eq. (3).

$$w_1 = \gamma + / T_{services} \tag{3}$$

While w_2 denotes the weight of direct trust, w_3 is equivalent to Θ^i, where i signifies the $i\tau b$ trust guarantee for device recommendation. It is crucial to note that 0 is less than or equal to 1. As the quantity of services I appreciate expands, so too does the proliferation of those services. To establish a connection with other devices, a node v must first attain a designated threshold trust level, represented by the symbol T. A connection will be acknowledged if the computed trust value exceeds T. Diverse applications can utilise various values of T. Conversely, in this specific experiment, we have utilised solely dual values.

The IIWOADL-TMS model enhances trust evaluation accuracy by incorporating a hybrid trust assessment framework that combines direct and indirect trust factors. By integrating historical behavior, service quality, peer recommendations, and reputation analysis, the model ensures a robust and dynamic trust computation mechanism for secure SIoT environments.

Trust Computation Formula in IIWOADL-TMS.

The Total Trust Value (TTVL) of a device is computed as:

$$\text{TTVL} = \alpha T_{\text{direct}} + \beta T_{\text{indirect}} + \gamma T_{\text{recommendation}}$$

where: $T_{\text{direct}} \rightarrow$ Trust score from direct interactions; $T_{\text{indirect}} \rightarrow$ Trust score from aggregated reputation and network observations; $T_{\text{recommendation}} \rightarrow$ Trust score from peer recommendations; α, β, $\gamma \rightarrow$ Weight factors assigned to each trust component.

If TTVL < Threshold Value (THVL), the device is considered untrustworthy, and access is denied.

3.2 LSTM-Based Threshold Value Selection

The IIWOADL-TMS method employs LSTM to dynamically verify the THVL for site visitors facts collection. Output, enter, and neglect gates are the 3 gates commonly incorporated in an LSTM. The enter gate is the major determinant of ways memory cells are regulated, with the modern-day input.

The estimation is finished using the following formulation:

The input gate feature is expressed as: The input activation is decided via making use of the sigmoid feature to the weighted sum of the previous hidden state and the current input, at the side of a bias term. The cellular state update is given with the aid of: A candidate cell state is generated by applying the hyperbolic tangent feature to the weighted aggregate of the previous hidden country and current enter, plus a bias. The forgot gate basically determines which facts within the preceding reminiscence cellular must be forgotten. In most instances, the activation feature of the sigmoid feature is essentially motivated by using the previous cellular state.

The method describing the overlook gate's operation is supplied below:

The forget gate function, makes a decision on how an awful lot of records from the preceding state have to be retained or forgotten through making use of the sigmoid characteristic to the weighted mixture of the preceding hidden state and the modern input, alongside a bias term. The output gate is the key element governing the go with the flow of statistics from the present reminiscence cell to the hidden layer.

The output gate function: This determines the output activation with making use of the sigmoid characteristic to the weighted sum of the previous hidden state and the modern-day input, plus a bias.

The hidden state update: The updated hidden country is acquired through multiplying the output gate activation with the hyperbolic tangent of the cutting-edge cell nation. This design ensures that the system maintains consistency irrespective of the quantity of input information, whether or not huge or small. Additionally, it enables the device to adaptively modify its activation nation based totally on varying input situations. The LSTM version is illustrated in Fig. 2.

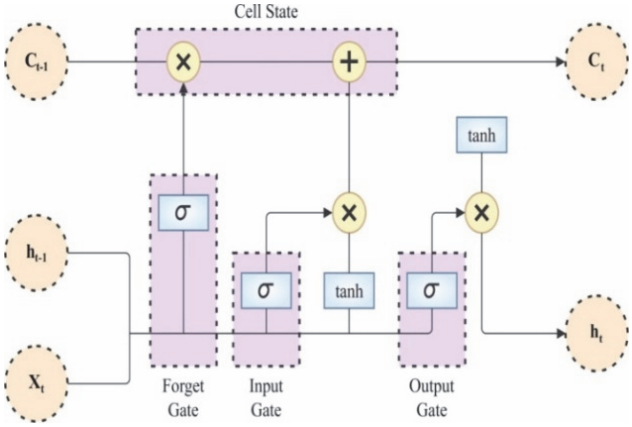

Figure 2 Structure of LSTM model

3.3 IWOA-Based Hyperparameter Tuning Method

To attain optimal hyperparameter tuning of the LSTM system, the IIWOADL-TMS model outperforms the IWOA method. A unique optimisation method called WOA [20] was created, inspired by the searching behaviour of humpback whales. Whales employ the bubble-net hunting technique to ensnare and encircle progressively larger groups of fish. The ideal hunting position for whales is at prey site X, but the capacity of other whales to enhance their location is contingent upon X. Whales exhibit three behaviours: encircling their prey, exploiting it, and examining it.

3.4 Encircling Prey

During foraging, whales may also detect their prey and surround them. This enhances their chance of fulfillment. Currently, the most advantageous whale, denoted as X, is seemed as prey or is nearer to being prey. X updates the places of all different whales primarily based on the following steps:

1. Calculate the distance D among the whale and the prey - D is determined with the aid of taking absolutely the distinction among the fabricated from coefficient C and the

prey's function X at time t, and the whale's function X at time t.

2. Update the whale's role - the brand new role of the whale at $t + 1$ is received by means of subtracting the fabricated from coefficient A and distance D from the prey's function X at time t.

In this computation: t represents the iteration counter. $X(t)$ denotes the location of a whale at iteration t. $X(t)$ represents the placement of the prey. A and C are coefficient vectors. The coefficients A and C are computed as follows: A is calculated using the components: $2 \times a \times r - a(t)^2$ times a instances $r - a(t)$, where a decreases linearly from 2 to 0 and r is a random wide variety among 0 and 1. C is given by: $2 \times r^2$ instances r, where r is randomly decided on within the variety [0, 1].

3.5 Bubble-Net Attacking

To facilitate the motion of whales round their prey, a spiral update method is hired. The behaviors of the whales are adjusted primarily based on the following situations: If the probability p is less than 0.5, the diminishing encircling mechanism is used, where the whale updates its position by the use of the approach described inside the encircling prey phase. If p is more than or equal to 0.5, the spiral updating approach is implemented, wherein the whale's function is changed by the use of a spiral equation that includes the exponential feature, cosine function, and a distance element. In this context, p is a randomly generated quantity in the variety [0, 1]. A random c language is generated in the variety $[-a, a]$, even as a regularly decreases from 2 to 0. D' represents the space among the prey X and the whale X at the place of the spiral update. B is a regular that defines the shape of the spiral motion. L is randomly selected in the variety $[-1, 1]$. This method permits whales to both circle inwards toward the prey or use spiral actions to achieve their goal, thereby improving their ability to seize prey efficaciously.

4 RESULTS AND DISCUSSION

This section offers a definitive validation of the simulation study performed on the IIWOADL-TMS methodology. The comparative analysis of the IIWOADL-TMS algorithm can be assessed under diverse parameters regarding delay (DEL) and packet delivery ratio (PDR) relative to the monitoring interval (MI) [22]. The findings of this investigation are illustrated in Tab. 1.

Table 1 Comparative outcomes of IIWOADL-TMS technique with other models

MI / s	IIWOADL-TMS	TAAPML	TMM
DEL / ms			
10	45.72	50.00	53.00
20	47.03	50.66	53.87
30	47.25	51.33	54.25
40	47.83	51.61	54.78
50	48.00	52.26	55.27
PDR			
10	98.30	98.12	98.31
20	98.55	98.40	98.69
30	98.69	98.57	99.12
40	98.73	98.60	99.34
50	98.79	98.68	99.97

Fig. 3 signifies a comparison DEL outcome of the IIWOADL-TMS method under several MIs. The figure specify that the TMM technique has exhibited worse results compared to methods. Likewise, the TAAPML approach has outperformed that somewhat lower value of DEL. Nevertheless, the IIWOADL-TMS methodology has demonstrates better performances with least DEL values of 35.72 ms, 37.03 ms, 37.25 ms, 38.83 ms, and 38 ms under MIs of 20 s - 100 s, respectively.

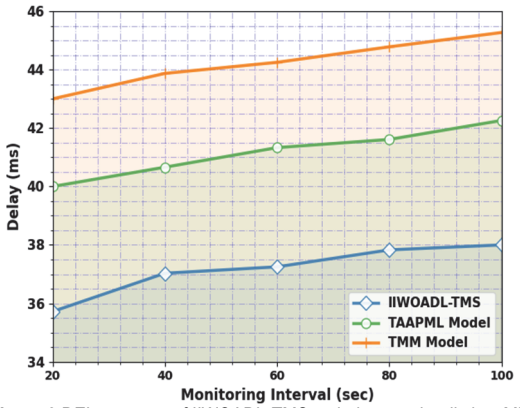

Figure 3 DEL outcome of IIWOADL-TMS technique under distinct Mis

A brief PDR study of the IIWOADL-TMS algorithm with current methods under distinctive MIs is specified in Fig. 4. The figure exhibits that the IIWOADL-TMS methodology has got higher result with higher values of PDR. With MI of 20 s, the IIWOADL-TMS model provides better PDR value of 99.30 whereas the TAAPML model and TMM technique reach lower PDR values of 99.12 and 97.31 respectively. Moreover, with MI of 80 s, the IIWOADL-TMS system provides greater PDR of 99.73 whereas the TAAPML approach and TMM methodology achieve the least PDR of 99.60 and 98.34 respectively.

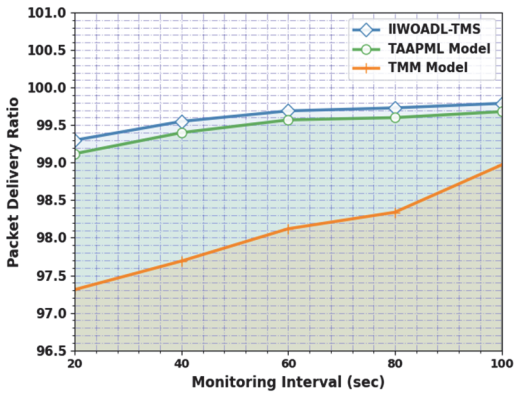

Figure 4 PDR outcome of IIWOADL-TMS technique under various Mis

The comparative study of the IIWOADL-TMS technique is examined based on residual energy (RSE) and overhead (OHD) with respect to MI. Fig. 5 offers a complete RSE analysis of the IIWOADL-TMS model with current approaches under various MIs. The results show that the IIWOADL-TMS approach has displayed improved fallouts with superior values of RSE. For example, with MI of 20 s, the IIWOADL-TMS system has accomplished higher RSE of 11.79 J whereas the TAAPML system and TMM method have got reduced RSE of 11.66 J and 11.41 J respectively. Also, with MI of 100 s, the IIWOADL-TMS methodology has attained improved RSE of 10.68 J but the

TAAPML algorithm and TMM approach have stated lower RSE of 10.44 J and 10.28 J respectively.

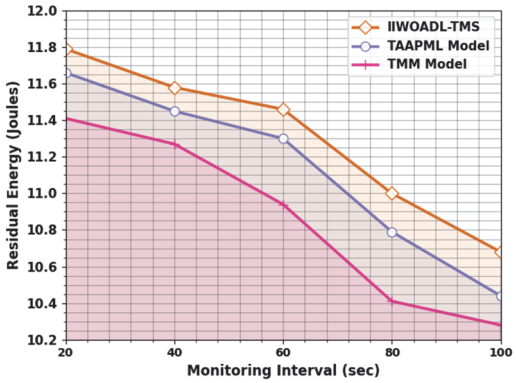

Figure 5 RSE outcome of IIWOADL-TMS system under various MIs

Fig. 6 denotes a comparable OHD outcome of the IIWOADL-TMS method under different MIs. The outcome specifies that the TMM technique has exhibited worse outcomes compared to methods. Likewise, the TAAPML approach has outperformed the somewhat decreased value of DEL. However, the IIWOADL-TMS methodology has demonstrated better performances with the least OHD values of 110 Kb, 229 Kb, 291 Kb, 401 Kb, and 121 Kb under MIs of 20 s - 100 s, respectively.

Fig. 7 denotes a comparative DEL outcome of the IIWOADL-TMS methodology under several attack frequencies (AFs). The outcome specifies that the TMM technique has exhibited worse results compared to the methods. Likewise, the TAAPML approach has outperformed the slightly lower value of DEL. Nevertheless, the IIWOADL-TMS methodology has demonstrated better performances with the least DEL values of 38.09 ms, 37.81 ms, 37.12 ms, 37.05 ms, and 38 ms under AF of 50 Kb - 150 Kb, respectively.

A brief PDR study of the IIWOADL-TMS method with current techniques under diverse AFs is provided in Fig. 8. The results exhibit that the IIWOADL-TMS system has attained enhanced performance with superior values of PDR. With AF of 50, the IIWOADL-TMS methodology obtains better PDR value of 99.95 whereas the TAAPML system and TMM approach gained lower PDR values of 99.91 and 99.09 respectively. Also, with AF of 150 Kb, the IIWOADL-TMS method provides improved PDR of 98.35 whereas the TAAPML approach and TMM system attain reduced PDR values of 98.15 and 96.96 respectively.

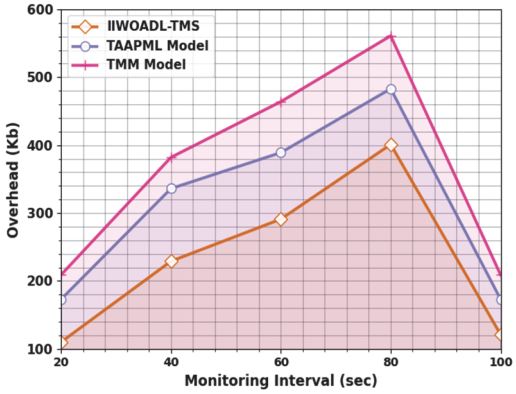

Figure 6 IIWOADL-TMS method results at different MIs

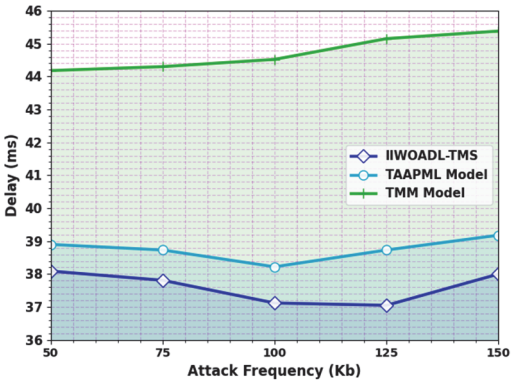

Figure 7 DEL results of the IIWOADL-TMS method with different AFs

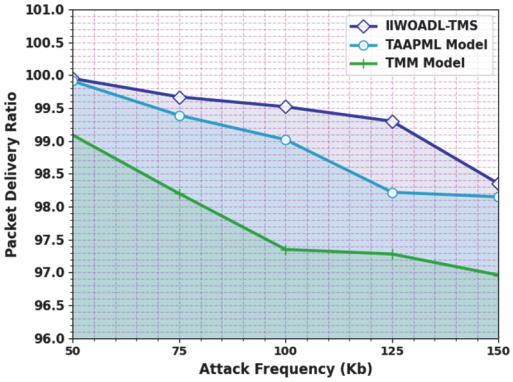

Figure 8 PDR results using the IIWOADL-TMS algorithm at different AFs

Table 2 Outcomes of IIWOADL-TMS technique with other models

AF / Kb	IIWOADL-TMS	TAAPML	TMM
RES / J			
10	12.12	11.08	11.76
25	12.29	12.21	11.97
50	12.31	12.27	11.87
100	12.39	12.27	12.17
125	12.40	12.30	12.20
OHD / Kb			
10	62	88	146
25	108	138	246
50	143	180	334
100	191	234	378
125	203	280	454

Tab. 2 gives the comparison examination of the IIWOADL-TMS system based on RES and OHD in terms of AF.

Fig. 9 offers a comprehensive RSE examination of the IIWOADL-TMS system with present methods under various AFs. The results show that the IIWOADL-TMS system has displayed improved results with greater values of RSE. For example, with AF of 50 Kb, the IIWOADL-TMS model has accomplished the greatest RSE of 11.02 J whereas the TAAPML and TMM methods have got reduced RSE of 10.98 J and 10.66 J respectively. Also, with AF of 150 Kb, the IIWOADL-TMS algorithm has attained better RSE of 11.30 J but the TAAPML approach and TMM system have reported minimal RSE of 11.20 J and 11.10 J respectively.

Fig. 10 signifies a comparison OHD outcome of the IIWOADL-TMS model at distinct AFs. The outcome specifies that the TMM technique has exhibited worse outcome compared to methods. Likewise, the TAAPML approach has outperformed that slightly lower value of DEL. However, the IIWOADL-TMS methodology has demonstrated better performances with least OHD values

of 61 Kb, 106 Kb, 141 Kb, 189 Kb, and 201 Kb under AF of 50 Kb - 150 Kb, respectively.

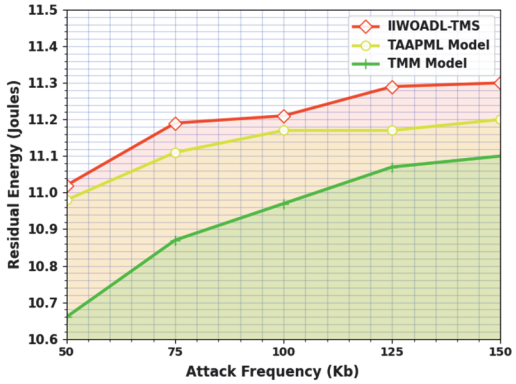

Figure 9 Examination of the IIWOADL-TMS methodology at different AFs

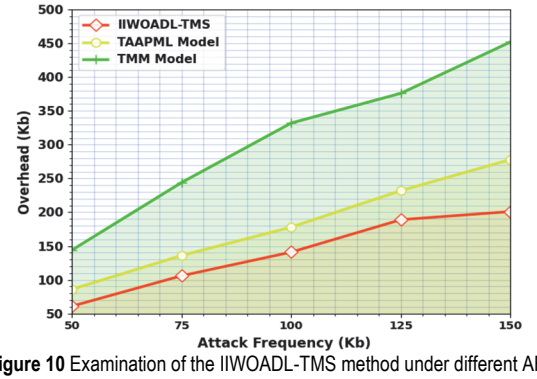

Figure 10 Examination of the IIWOADL-TMS method under different AFs

5 CONCLUSION

We have built an IIWOADL-TMS model for application in the SIoT Network, which is described in this paper. The IIWOADL-TMS system calculates both indirect and direct trust levels, with its performance assessed through various evaluation criteria. This is executed to enhance the application's overall performance and to establish a secure data transmission protocol. During authentication, the gateway will exclude the node if the TTVL of the SIoT device is below the THVL. The LSTM method can be employed to develop a THVL based on the compiled traffic data during the classification process. The IWOA method is employed by the IIWOADL-TMS technique to ascertain the appropriate hyperparameter range for the LSTM system. The experimental validation of the IIWOADL-TMS approach and the simulation analysis indicate that the IIWOADL-TMS strategy outperforms other models. The experimental validation was conducted under various conditions.

Acknowledgments

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R387), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2025R787), King Saud University, Riyadh, Saudi Arabia.

6 REFERENCES

[1] Azad, M. A., Bag, S., Hao, F., & Shalaginov, A. (2020). Decentralized self-enforcing trust management system for social Internet of Things. *IEEE IoT Journal*, *7*(4), 2690-2703. https://doi.org/10.1109/JIOT.2019.2962282

[2] Velumani, R. & Kalimuthu, V. K. (2023). Barnacles Mating Optimizer with Hopfield Neural Network-Based Intrusion Detection in IoT Environment. *Tehnički vjesnik*, *30*(6), 1821-1828. https://doi.org/10.17559/TV-20230414000533

[3] Abuagoub, A. M. (2019). IoT security evolution: Challenges and countermeasures review. *International Journal of Communication Networks and Information Security*, *11*(3), 342-351. https://doi.org/10.17762/ijcnis.v11i3.4272

[4] Garg, S., Kaur, K., Kaddoum, G., Ahmed, S. H., & Jayakody, D. N. K. (2019). SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective. *IEEE Transactions on Vehicular Technology*, *68*(9), 8421-8434. https://doi.org/10.1109/TVT.2019.2917776

[5] Xiang, X., Cao, J., Fan, W., Xiang, S., & Wang, G. (2024). Blockchain-enabled dynamic trust management method for the Internet of Medical Things. *Decision Support Systems*, 180, 114184. https://doi.org/10.1016/j.dss.2024.114184

[6] Souri, A., Zhao, Y., Gao, M., Mohammadian, A., Shen, J., & Al-Masri, E. (2023). A trust-aware and authentication-based collaborative method for resource management of cloud-edge computing in social Internet of Things. *IEEE Transactions on Computational Social Systems*, *11*(4), 4899-4908. https://doi.org/10.1109/TCSS.2023.3241020

[7] Rizwanullah, M., Singh, S., Kumar, R., Alrayes, F. S., Alharbi, A., Alnfiai, M. M., Chaurasia, P. K., & Agrawal, A. (2022). Development of a model for trust management in the social Internet of Things. *Electronics*, *12*(1), 41. https://doi.org/10.3390/electronics12010041

[8] Vinoth Kumar, K. & Rajakani, V. (2024). Modeling of Intrusion Detection System using Double Adaptive Weighting Arithmetic Optimization Algorithm with Deep Learning on Internet of Things Environment. *Brazilian Archives of Biology and Technology*, *67*, e24231010. https://doi.org/10.1590/1678-4324-2024231010

[9] Amiri-Zarandi, M., Dara, R. A., & Fraser, E. (2022). LBTM: A lightweight blockchain-based trust management system for social Internet of Things. *The Journal of Supercomputing*, *78*, 8302-8320. https://doi.org/10.1007/s11227-021-04231-3

[10] Tahir, M., Sardaraz, M., Muhammad, S., & Saud Khan, M. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics. *Sustainability*, *12*(17), 6960. https://doi.org/10.3390/su12176960

[11] Abdelghani, W., Amous, I., Zayani, C. A., Sèdes, F., & Roman-Jimenez, G. (2022). Dynamic and scalable multi-level trust management model for Social Internet of Things. *The Journal of Supercomputing*, *78*(6), 8137-8193. https://doi.org/10.1007/s11227-021-04205-5

[12] Magdich, R., Jemal, H., & Ayed, M. B. (2022). A resilient trust management framework towards trust related attacks in the social Internet of Things. *Computer Communications*, *191*, 92-107. https://doi.org/10.1016/j.comcom.2022.04.006

[13] Magdich, R., Jemal, H., & Ayed, M. B. (2022). Context-awareness trust management model for trustworthy communications in the social Internet of Things. *Neural Computing and Applications*, *34*(24), 21961-21986. https://doi.org/10.1007/s00521-022-07656-w

[14] Bangui, H., Buhnova, B., Kusnirakova, D., & Halasz, D. (2023). Trust management in social IoTacross domains. *Internet of Things*, *23*, 100833. https://doi.org/10.1016/j.iot.2023.100833

[15] Latif, R. (2022). ConTrust: A novel context-dependent trust management model in social Internet of Things. *IEEE Access*, *10*, 46526-46537. https://doi.org/10.1109/ACCESS.2022.3169788

[16] Roy, S. S., Sahu, B. J. R., & Dash, S. (2023). Enhanced trust management for building trustworthy social IoT network. *IET Networks*, *14*(1), e12111. https://doi.org/10.1049/ntw2.12111
[17] Zhang, H., Fan, F., Zhao, D., Liu, B., Wang, Y., & Liu, J. (2022). Social IoT trust management based on implicit social relationship. *International Conference on Security and Privacy in New Computing Environments*, 129-139. https://doi.org/10.1007/978-3-031-30623-5_9
[18] Wu, Y., Xiang, C., Qian, H., & Zhou, P. (2024). Optimization of Bi-LSTM photovoltaic power prediction based on improved snow ablation optimization algorithm. *Energies*, *17*(17), 4434. https://doi.org/10.3390/en17174434
[19] Vinaykumar, V. N., Babu, J. A., & Frnda, J. (2023). Optimal guidance whale optimization algorithm and hybrid deep learning networks for land use land cover classification. *EURASIP Journal on Advances in Signal Processing*, *2023*(1), 13. https://doi.org/10.1186/s13634-023-00980-w
[20] Jia, G., Meng, Y., & Qin, Z. (2024). Bearing fault diagnosis based on optimized feature mode decomposition and improved deep belief network. *Structural Durability & Health Monitoring (SDHM)*, *18*(4), 445-463. https://doi.org/10.32604/sdhm.2024.049298
[21] Chinnaswamy, S. & Annapurani, K. (2021). Trust aggregation authentication protocol using machine learning for IoT wireless sensor networks. *Computers & Electrical Engineering*, *91*, 107130. https://doi.org/10.1016/j.compeleceng.2021.107130

Contact information:

Kavitha RAVICHANDRAN, Assistant Professor
(Corresponding author)
Department of Computer Science and Engineering,
University College of Engineering BIT Campus,
Anna University, Tiruchirappalli, India
E-mail: kavitha.r152024@gmail.com

Murugesan GURUSAMY, Associate Professor
Department of Electronics and Communication Engineering,
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, India

Ghadah ALDEHIM
Department of Information Systems,
College of Computer and Information Sciences,
Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

Mashael MAASHI
Department of Software Engineering,
College of Computer and Information Sciences,
King Saud University, Po box 103786, Riyadh 11543, Saudi Arabia