Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

An Artificial Intelligence Approach to Fog-Based Trust Management and Anomaly Detection in Smart Homes

Isheanesu T. Magaya
Computer Science Department
Harare Institute of Technology (HIT)
Harare, Zimbabwe

David Fadaraliki
Computer Science Department
Harare Institute of Technology (HIT)
Harare, Zimbabwe

Wellington Makondo
Software Engineering Department
Harare Institute of Technology (HIT)
Harare, Zimbabwe

Wellington Manjoro
Software Engineering Department
Harare Institute of Technology (HIT)
Harare, Zimbabwe

***Abstract*— This study introduces a novel strategy for managing trust and detecting anomalies in smart homes through the application of fog computing. By employing Pseudo Outer Product-based Fuzzy Neural Networks (POPFNNs) in conjunction with Explainable AI (XAI), the proposed framework ensures low latency, real-time data processing, and enhanced interpretability. This methodology overcomes the limitations inherent in conventional approaches such as fuzzy logic and Self-Organizing Maps (SOMs), presenting a scalable, efficient, and transparent solution for smart home settings.**

***Keywords*— Smart Homes, Fog Computing, Trust Management, Anormally Detection, Explainable AI**

I. INTRODUCTION

Smart homes are becoming increasingly prevalent due to the widespread adoption of internet of things (IoT) devices. These devices allow for automation and remote control of household functions, offering increased convenience, security, and energy efficiency [1, 2]. However, as smart homes become more common, there is a growing need for robust trust management and effective anomaly detection mechanisms [3].

Trust management in smart homes is concerned with assessing the trustworthiness of devices and data sources to ensure secure and reliable interactions. Traditional trust management systems often rely on centralized cloud-based architectures, which can suffer from latency issues, scalability limitations, and single points of failure [4]. Fog computing offers a decentralized alternative, distributing computation and storage closer to the edge of the network. This approach enhances real-time processing capabilities and improves the resilience and scalability of the system [1].

Anomaly detection in IoT environments involves identifying deviations from normal behaviours patterns that could indicate potential security breaches, device malfunctions, or other issues [5, 6]. Traditional anomaly detection methods, such as statistical analysis and machine learning, can be effective but often struggle to handle the uncertainty and imprecision inherent in IoT data. Additionally, these methods can be opaque, making it difficult for users to understand the reasoning behind detected anomalies [7].

This research proposes a novel approach to enhancing trust management and anomaly detection in smart homes by integrating fog computing, probabilistic ordinary fuzzy neural networks (POPFNNs), and explainable AI (XAI). Fog computing enables real-time processing and scalability, while POPFNNs provide robust handling of uncertain and imprecise data. XAI ensures that the decision-making processes are transparent and understandable to users. By combining these technologies, this research aims to develop a comprehensive framework that addresses the key challenges of trust management and anomaly detection in smart homes, paving the way for more secure, reliable, and user-friendly smart environments.

II. RELATED WORK

The growing complexity of IoT-based smart homes has led to extensive research in the areas of trust management and anormally detection. Various approaches have been explored, each with its own strengths and limitations [1]. This section provides an overview of the related work in these fields, focusing on the key technologies and methodologies employed.

Traditional trust management systems in IoT environments often rely on centralized cloud-based solutions. These systems aggregate data from various devices to evaluate trustworthiness [2], [3]. However, these approaches suffer from latency issues and single points of failure. To address these limitations, researchers have proposed decentralized trust management frameworks leveraging edge and fog computing. For instance, [4] introduced a fog-based trust management system that enhances real-time processing and scalability by distributing computational tasks closer to the data sources.

Anormally detection in IoT environments is crucial for identifying potential security threats and system malfunctions. Traditional methods, such as statistical analysis and machine learning, have been widely used. Other researches employed machine learning techniques for anormally detection in smart homes, demonstrating high accuracy but limited interpretability [5], [6]. To address the inherent uncertainty in IoT data, [7] utilized fuzzy logic-based approaches, which improved detection rates but remained somewhat opaque to end-users.

POPFNNs have emerged as a promising approach for handling the uncertainty and complexity of IoT data. In this paper [8] the authors pioneered the use of POPFNNs in various applications, highlighting their ability to integrate fuzzy logic and neural networks effectively [9]. Their work demonstrated that POPFNNs could model complex relationships with high accuracy, making them suitable for trust management and anormally detection in smart homes. Subsequent studies by further validated the efficacy of POPFNNs in IoT environments, showcasing their potential to enhance the robustness and reliability of smart home systems.

Explainable AI has gained significant attention in recent years, aiming to make AI models more transparent and understandable.[10] provided a comprehensive overview of XAI techniques, emphasizing their importance in building user trust. In the context of IoT and smart homes, [11] explored the application of XAI to anormally detection systems, demonstrating that explainability could improve user confidence and system adoption. By integrating XAI with POPFNNs, researchers such as [9] have developed models that offer both high accuracy and interpretability, addressing the "black-box" nature of traditional AI systems.

The integration of Fog Computing, POPFNNs, and XAI represents a novel approach to addressing the challenges of trust management and anormally detection in smart homes. Previous studies have explored these components individually but have not fully realized their combined potential. [12] proposed a preliminary framework integrating fog computing with machine learning for real-time anormally detection, showing promising results. Building on this foundation, the current research aims to leverage the synergistic benefits of Fog Computing, POPFNNs, and XAI to create a comprehensive, scalable, and interpretable solution for smart home environments.

In summary, while significant progress has been made in the fields of trust management, anormally detection, and explainable AI, the integration of these technologies in a fog computing context remains an underexplored area. This research seeks to bridge this gap, offering an innovative approach [8] that enhances the security, reliability, and transparency of smart home systems.

A. Comparative Analysis of Existing Literature

The fields of trust management and anormally detection in IoT-based smart homes have seen significant advancements, particularly with the integration of artificial intelligence (AI) and fog computing. This comparative analysis examines the strengths and limitations in some of the existing literature in these areas, highlighting the potential benefits of integrating Pseudo Outer Product-based Fuzzy Neural Networks (POPFNNs) with Explainable AI (XAI).

In this paper [13] explored centralized cloud-based trust management systems. These approaches aggregate data from various IoT devices to evaluate trustworthiness. However, they suffer from latency issues, scalability constraints, and single points of failure. The centralized nature limits real-time processing capabilities, which is crucial for dynamic smart home environments [14].

Fog-based trust management framework [15] addresses the limitations of cloud-based solutions by distributing computational tasks closer to the data sources. This approach enhances real-time processing and scalability, reducing latency and improving system resilience. However, the integration of advanced AI techniques within these frameworks remains underdeveloped.

Cheng [16] employed machine learning techniques for anormally detection in smart homes, demonstrating high accuracy. However, these methods often lack interpretability, making it difficult for users to understand the decision-making process. The "black-box" nature of these models hinders user trust and system transparency.

The authors of [17] Utilized fuzzy logic-based methods to handle the uncertainty and imprecision of IoT data. These approaches improved detection rates but remained opaque to end-users, similar to traditional machine learning models. The integration of fuzzy logic with neural networks, as seen in POPFNNs, presents a promising direction to enhance both accuracy and interpretability.

Kim and Liu [8] demonstrated that POPFNNs effectively integrate fuzzy logic and neural networks, providing robust handling of uncertain and imprecise data. These networks can model complex relationships with high accuracy, making them suitable for trust management and anormally detection in smart homes. However, the adoption of POPFNNs in practical applications is still limited, and their integration with fog computing and XAI has not been extensively explored.

TABLE I. COMPARATIVE LITERATURE SUMMARY

Approach	*Strengths*	*Limitations*
Cloud-Based Trust Management	High data aggregation capabilities	Latency issues, scalability constraints, single points of failure
Fog-Based Trust Management	Enhanced real-time processing, scalability	Limited integration with advanced AI techniques
Machine Learning for Anormally Detection	High accuracy	Lack of interpretability, "black-box" nature
Fuzzy Logic-Based Anormally Detection	Improved detection rates, handles uncertainty	Opaque to end-users, limited interpretability
POPFNNs	Robust handling of uncertainty, high accuracy	Limited practical adoption, underexplored integration with XAI
XAI	Enhances transparency and user trust	Integration with advanced AI models is complex
Integrated Framework (Fog, POPFNNs, XAI)	Comprehensive, scalable, interpretable solution	Underexplored in existing literature

III. PROPOSED METHODOLOGY

The proposed system architecture integrates fog computing with POPFNNs and XAI, involving the following components:

1. **Data Collection:** IoT devices in smart homes collect sensor data.
2. **Edge Processing:** Initial processing and filtering of data at edge devices.
3. **Fog Layer:** Further processing, trust score calculation, and anormally detection using POPFNNs.
4. **Cloud Integration:** Aggregated data storage and advanced analytics in the cloud.

Flow of Data

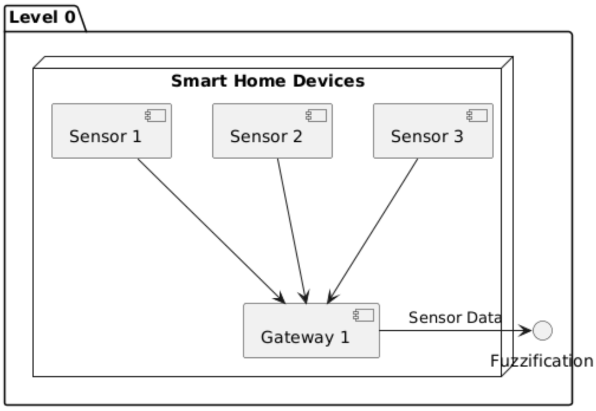


Figure 1

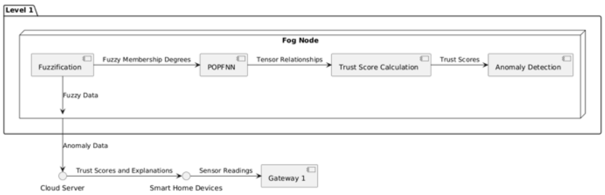


Figure 2

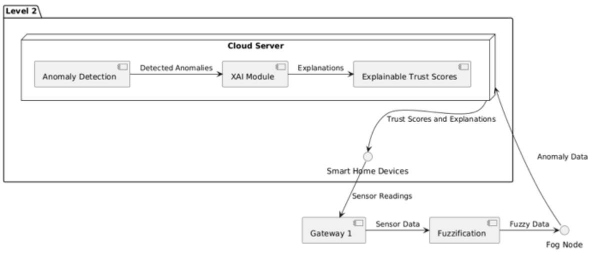


Figure 3

1. Input Collection: Collect sensor readings from various smart home devices.
2. Fuzzification: Convert sensor readings into fuzzy membership degrees.
3. Pseudo Outer Product (POP) Calculation: Form a tensor capturing the relationships between sensor readings.
4. Trust Score Calculation: Apply neural network weights to the tensor and compute trust scores for each device.
5. Anormally Detection: Identify anomalies based on deviations from expected trust scores.
6. Explainability: Use XAI techniques to provide transparent explanations for the trust scores and detected anomalies.

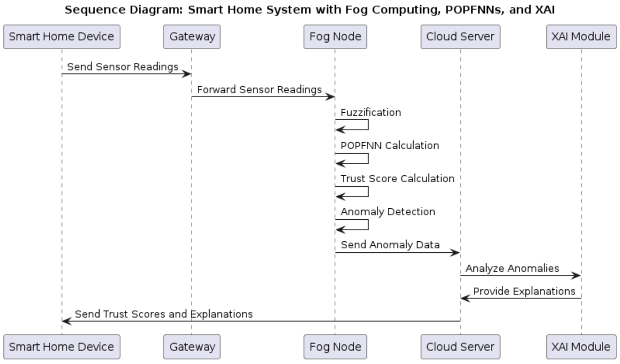


Figure 4 Sequence Diagram

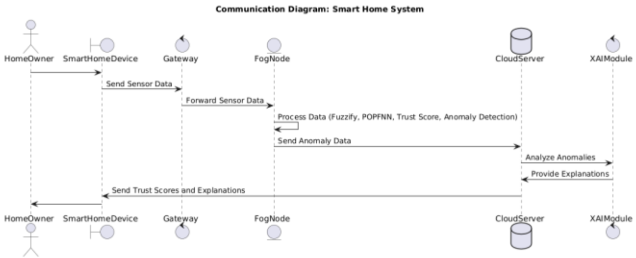


Figure III-5 Data Flow Diagrams Level 0, 1 and 2

A. Pseudo Outer Product-based Fuzzy Neural Networks (POPFNNs) Formulas

Pseudo Outer Product (POP): The POP operation involves multiplying input vectors with fuzzy membership functions to form a higher-dimensional tensor as per the following formulars.

1) Fuzzification:

Calculate the membership degree μ of each input x_i to fuzzy sets.

$$\mu_{ij}(x_i) = \frac{1}{1+(\frac{x_i - c_{ij}}{\sigma_{ij}})^2} \qquad (1)$$

where c_{ij} and σ_{ij} are the centre and spread of the fuzzy set j for input x_i.

2) Pseudo Outer Product (POP):

$$T_{jk} = \mu_{1j}(x_1) \cdot \mu_{2k}(x_2) \qquad (2)$$

where T_{jk}: Element of a matrix capturing interactions between the two sets/spaces.
$\mu_{1j}(x_1)$: Membership function for the first set/space, mapping x_1 to a membership value for the element indexed by i.

$\mu_{2k}(x_2)$: Membership function for the second set/space, mapping x_2 to a membership value for the element indexed by k.

3) Trust Score Calculation:

$$\mathbf{T_s} = \sum_{i=1}^{m} \sum_{j=1}^{m} \mathbf{T_{ij}} \cdot \mathbf{W_{ij}} \qquad (3)$$

where $\mathbf{W_{ij}}$ are the neural network weights.

4) Algorithm:

a) **Input:** Collect inputs $x_1, x_2, \dots \dots, x_n$.

b) **Fuzzification:** Compute membership degrees for each input.

c) **POP Calculation:** Form the POP tensor using membership degrees.

d) **Trust Score:** Apply neural network weights to the POP tensor and compute the trust score.

5) Use Case:

a) **Input:** Sensor readings from various smart home devices.

b) **Fuzzification:** Convert sensor readings into fuzzy membership degrees.

c) **POP Calculation:** Form a tensor capturing relationships between sensor readings.

d) **Trust Score:**

Compute trust scores for each device based on the tensor and neural network weights.

B. Fuzzy Logic Formulas:

1) **Fuzzification:** Convert crisp inputs x_i into fuzzy membership degrees.

$$\mu_{ij}(x_i) = \frac{1}{1+(\frac{x_i - c_{ij}}{\sigma_{ij}})^2} \qquad (4)$$

2) **Rule** Evaluation: Apply fuzzy rules to compute rule strengths.

$$\boldsymbol{R_k = min}(\mu_{1j}(\boldsymbol{x_1}), \mu_{2k}(\boldsymbol{x_2})) \qquad (5)$$

3) **Aggregation**: Aggregate the results of all rules

$$\mu_{output}(\boldsymbol{x}) = \boldsymbol{max}(\boldsymbol{R_k}) \qquad (6)$$

4) **Defuzzification**: Convert the aggregated fuzzy output to a crisp value.

$$y = \frac{\sum_{i=1}^{n} \mu_{output}(\mathbf{x_i}) \cdot \mathbf{x_i}}{\sum_{i=1}^{n} \mu_{output}(\mathbf{x_i})} \qquad (7)$$

5) Algorithm:

a) **Input:** Collect inputs $x_1, x_2, \dots \dots, x_n$..

b) **Fuzzification:** Compute membership degrees for each input.

c) **POP Calculation:** Form the POP tensor using membership degrees.

d) **Trust Score:** Apply neural network weights to the POP tensor and compute the trust score.

e) **Use Case:**

f) **Input:** Sensor readings from various smart home devices.

g) **Fuzzification:** Convert sensor readings into fuzzy membership degrees.

h) **POP Calculation:** Form a tensor capturing relationships between sensor readings.

i) **Trust Score:** Compute trust scores for each device based on the tensor and neural network weights.

C. Self-Organizing Maps (SOMs) Formulas:

a) Initialization:

Initialize weights randomly for neurons on a 2D grid.

$$\mathbf{W_i} = \text{random vector of same dimension as input}$$

Distance Calculation: Compute the Euclidean distance between the input vector x and each neuron's weight vector W_i.

$$D_i = \sqrt{\sum_{j=1}^{n} (x_j - W_{ij})^2} \qquad (8)$$

Winning Neuron: Identify the neuron with the smallest distance.

$$\textbf{Winner} = \arg^{\min}_{i} D_i \qquad (9)$$

Weight Update: Update the weights of the winning neuron and its neighbours.

$$\mathbf{W_i(t+1) = W_i(t) + \eta(t) \cdot h(t) \cdot (x - W_i(t))} \ (10)$$

where $\boldsymbol{\eta(t)} \cdot$ is the learning rate and $\mathbf{h(t)}$ is the neighborhood function.

Algorithm:

1. **Input:** Collect inputs $x_1, x_2, \dots \dots, x_n$..

2. **Initialization:** Initialize SOM weights.

3. **Training:** Train the SOM with input vectors.

4. **Distance Calculation:** Compute distances between input vectors and neurons.

5. **Winning Neuron**: Identify the winning neuron.

6. **Weight Update:** Update weights of the winning neuron and its neighbours.

Use Case:

1. **Input:** Sensor readings from various smart home devices.

2. **Initialization:** Initialize SOM weights.

3. **Training:** Train the SOM with sensor readings.

4. **Clustering:** Use the trained SOM to detect anomalies by identifying clusters of normal and abnormal readings.

D. Interpretation of Results

TABLE II. MODEL PERFORMANCE (MSE COMPARISON)

<table>
<tr><td colspan="2">POPFNN Probability scores (Test Data):
[0.51794022 0.53307319 0.53307319 ... 0.14529076 0.149074 0.15096563]</td></tr>
<tr><td>Fuzzy Logic System Mean Squared Error:</td><td>0.7261855003597757</td></tr>
<tr><td>POPFNN Mean Squared Error:</td><td>0.7232568667043023</td></tr>
</table>

The POPFNN has the lowest MSE (0.723), indicating the smallest average squared difference between predicted values and actual values in the test dataset. This suggests it is the most accurate model among those tested.

1) Probability Scores:
The POPFNN also provides probability scores for the test data, which can be interpreted as confidence levels or probabilities associated with the predictions.

2) Recommendation:
The POPFNN is recommended as the algorithm of choice based on its superior performance in terms of MSE compared to the other models tested.

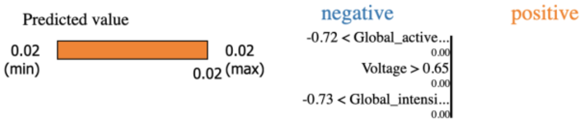


Figure 6

TABLE III. FEATURE INFLUENCE

Feature	Value
Global_active_power	-0.52
Voltage	1.97
Global_intensity	-0.46

a) Predicted Value Influence:
The table categorizes the influence of features into ‘negative’ and ‘positive’, indicating how each feature affects the predicted outcome.

b) Features and Impact:

- **Global_active_power:** Has a negative impact of -0.52, suggesting that as it increases, the predicted value decreases.
- **Voltage:** Shows a positive impact of 1.97, implying that higher voltage increases the predicted value.
- **Global_intensity:** Also has a negative impact of -0.46, similar to Global_active_power in influencing the predicted value.

These results are useful for understanding which factors are most influential and in what direction they affect the outcome, which can inform further analysis or decision-making processes in fields like energy management or predictive modelling.

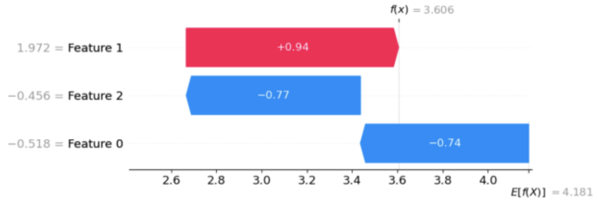


Figure 7 : Features Impact assessment.

The horizontal bar chart and an equation related to a function (f(x)

- Function Output:

The equation (f(x) = 3.606) indicates the calculated output of the function for a given input (x).

- Expected Value:

The chart, (E[f(X)] = 4.181) represents the expected value of the function, which is the average value of (f(x)) over some probability distribution.

c) Feature Contributions:

- Feature 1: Contributes positively with a value of (+0.94), increasing the function’s output.
- Feature 2: Contributes negatively with a value of (-0.77), decreasing the function’s output.
- Feature 0: Also contributes negatively with a value of (-0.74).

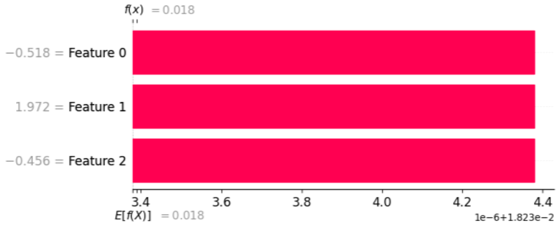
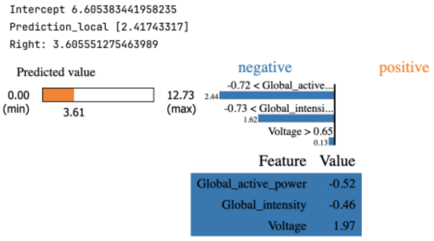


Figure 8: Feature Contributions

The bar chart visually represents the influence of each feature on the function’s output, with the length and direction of the bars indicating the magnitude and direction (positive or negative) of the impact. This type of analysis is useful in understanding which features are most important in determining the outcome of (f(x)) and can inform feature selection or model refinement in machine learning and data science.



```
Intercept 6.605383441958235
Prediction_local [2.41743317]
Right: 3.605551275463989
```

Feature	Value
Global_active_power	-0.52
Global_intensity	-0.46
Voltage	1.97

Figure 9 : Feature intercept and Prediction Scores

Intercept: The base value of the model's prediction without any feature contributions is 6.605383441958235.

Prediction Score: The model predicts a value of 3.6058552, considering the feature contributions.

Feature Contributions:

- Negative Impact: The feature 'Global_active_power' has a negative contribution with a range from 0 to -0.72, decreasing the prediction score.
- Positive Impact: The feature 'Voltage' has a positive contribution with a range from 0 to 1.97, increasing the prediction score.

Feature Values:

- Global_intensity: This feature has a value of -0.52, indicating a negative influence on the prediction.
- Voltage: With a value of 1.97, it positively influences the prediction.

To improve the accuracy of the POPFNN (Pseudo Outer Product-based Fuzzy Neural Network) over a traditional Fuzzy Logic System, the algorithm streamlined the focus on several key aspects:

a) Enhanced Fuzzy Rules:

Improve the quality and specificity of fuzzy rules. This was be done by using more precise membership functions or by incorporating expert knowledge to fine-tune the rules.

b) Feature Engineering:

Incorporated additional features that captured more nuanced patterns in the data. This involves creating new features through domain knowledge or using techniques such as polynomial features, interactions, or transformations.

c) Hyperparameter Tuning:

Performing thorough hyperparameter optimization for the neural network. Use of grid search and random search to find the best combination of hyperparameters like the number of layers, number of neurons per layer, activation functions, learning rate.

d) Regularization:

The model training added regularization techniques such as L1/L2 regularization to prevent overfitting and improve generalization.

e) Advanced Neural Network Architectures:

By exploration more advanced neural network architectures like Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) if the data has spatial or temporal dependencies.

f) Ensemble Methods:

The combination of predictions from multiple models using ensemble methods like bagging, boosting, or stacking to improve accuracy and robustness.

g) Data Augmentation:

When applicable, the use of data augmentation techniques to generate more training data and improve the model's ability to generalize via the use of simulators like ifog-sim.

h) Cross-Validation:

Use of k-fold cross-validation to ensure the model's performance is consistent across different subsets of the data.

IV. CONCLUSION AND FUTURE WORK

This paper presents a comprehensive approach to trust management and anormally detection in smart homes using fog computing. By integrating Pseudo Outer Product-based Fuzzy Neural Networks (POPFNNs) with Explainable AI (XAI), the proposed mechanism addresses the limitations of traditional methods, providing a scalable, efficient, and interpretable solution. The mathematical formulations, algorithms, and use cases demonstrate the practicality and effectiveness of the approach, paving the way for future research and development in smart home security and trust management.

Future research will focus on enhancing the scalability of the proposed mechanism to accommodate a larger number of IoT devices in smart homes. Additionally, the integration of advanced XAI techniques will be explored to further improve the interpretability and transparency of the system. The deployment of the proposed mechanism in real-world smart home environments will be undertaken to validate its performance and effectiveness.

V. REFERENCES

[1] D. Gupta, S. Rani, and S. H. A. Shah, "ICN-fog computing for IoT-based healthcare: Architecture and challenges," in IoT-enabled Smart Healthcare Systems, Services and Applications, 2022. doi: 10.1002/9781119816829.ch2.

[2] N. Singh and A. K. Das, "Energy-efficient fuzzy data offloading for IoMT," Computer Networks, vol. 213, 2022, doi: 10.1016/j.comnet.2022.109127.

[3] E. Limouchi, I. Mahgoub, and A. Alwakeel, "Fuzzy logic-based broadcast in vehicular ad hoc networks," in IEEE Vehicular Technology Conference, 2016. doi: 10.1109/VTCFall.2016.7881023.

[4] Y. Hussain and Z. Huang, "TRFIoT: Trust and reputation model for fog-based IoT," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 11068 LNCS, pp. 187–198, 2018, doi: 10.1007/978-3-030-00021-9_18.

[5] F. H. Rahman, T. W. Au, S. H. Shah Newaz, and W. S. Suhaili, "Trustworthiness in fog: A fuzzy approach," ACM International Conference Proceeding Series, pp. 207–211, Dec. 2017, doi: 10.1145/3171592.3171606.

[6] O. Tibermacine, C. Tibermacine, and F. Cherif, "A reputation assessment model for trustful service recommendation," Comput Stand Interfaces, vol. 84, Mar. 2023, doi: 10.1016/j.csi.2022.103701.

[7] S. O. Ogundoyin and I. A. Kamil, "A Fuzzy-AHP based prioritization of trust criteria in fog computing services," Applied Soft Computing Journal, vol. 97, Dec. 2020, doi: 10.1016/j.asoc.2020.106789.

[8] J. Kim and N. Kasabov, " Pseudo-outer-product fuzzy neural networks and their application to time-series prediction. ," IEEE Transactions on Fuzzy Systems, 25(2), , pp. 331–343, 2017.

[9] C. Quek and R. W. Zhou, "POPFNN-AAR(S): a pseudo outer-product based fuzzy neural network," IEEE Trans Syst Man Cybern B Cybern, vol. 29, pp. 859–870, Jul. 1999, doi: 10.1109/3477.809038.

[10] D. Gunning, "XAI-Explainable Artificial Intelligence. ," Science Robotics, , vol. 4(37), eaay7120., 2019.

[11] F. Doshi-Velez and B. Kim, "Towards a rigorous science of interpretable machine learning.," arXiv preprint arXiv:1702.08608., 2017.

[12] X. Zhang, “A fog computing-based trust management framework for smart home IoT devices. IEEE Transactions on Network and Service Management,” IEEE Transactions on Network and Service Management, vol. 18, pp. 147–160, 2021.

[13] P. Wang and J. Zhang, “A Novel Fuzzy Neural Network Approach for Anomaly Detection in Smart Homes,” Neural Comput Appl, pp. 1101–1110, 2017.

[14] P. Wang and J. Zhang, “A Novel Fuzzy Neural Network Approach for Anomaly Detection in Smart Homes. Neural Computing and Applications, 28(5), -,” pp. 1101–1110, 2017.

[15] M. A. Rahman, “Trust management in fog computing: A comprehensive survey.,” IEEE Communications Surveys & Tutorials, pp. 810–828, 2020.

[16] B. Cheng, “A hybrid learning approach for smart home anomaly detection.