A Fuzzy-Based Deep Kronecker Stacked Autoencoder for Attack Detection in Social IoT

Divya S.
Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India
divya.s@uvce.ac.in (corresponding author)

R. Tanuja
Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India
tanujar.uvce@gmail.com

Received: 15 April 2025 | Revised: 29 April 2025, 22 May 2025, and 3 June 2025 | Accepted: 6 June 2025

 DOI: https://doi.org/10.48084/etasr.11510

ABSTRACT

The Social Internet of Things (SIoT) combines the IoT and social networks. This paper introduces the Fuzzy Deep Kronecker Stacked Autoencoder (Fuzzy-DKSA), an innovative attack detection model tailored to security issues in the SIoT. The model employs Z-score normalization for consistent data scaling, followed by feature fusion using a Deep Neural Network (DNN) enhanced by the Gower similarity measure. The detection phase utilizes the strengths of the Deep Kronecker Network (DKN) and the Deep Stacked Autoencoder (DSA), incorporating fuzzy logic to dynamically adapt to various attack patterns and network conditions. The Fuzzy-DKSA model demonstrates impressive performance, achieving 92% accuracy, 91% F-score, and 91% precision, outperforming existing models such as GAN, MH-CNN-AM, TM-MLA, and HAD in attack detection capabilities, showcasing the potential of fuzzy logic in enhancing security solutions for SIoT.

Keywords-deep learning; Social Internet of Things (SIoT); malicious attacks; Deep Kronecker Network (DKN); intrusion detection

I. INTRODUCTION

The Social Internet of Things (SIoT) merges IoT technology with social networking principles, enhancing connectivity and user experiences. This innovative framework allows devices to interact in a socially aware manner, sharing information and collaborating based on their social context. Various types of ordinary devices can exchange data and information, such as sensors, processors, and software [1]. SIoT enables devices to participate in human-to-human data exchanges. This technology involves active systems that enhance network information sharing and community engagement [2]. The increased popularity of IoT devices has resulted in increasingly sophisticated attacks. These systems require enhanced security standards that go beyond standard operating procedures. Traditional methods and recent studies emphasize the integration of intelligent mechanisms, such as machine learning and anomaly detection, into updated measures to combat the progressively changing security challenges in SIoT environments [3]. The lack of resources in dynamic IoT networks leads signature-based and anomaly-based threat detection methods to ineffective operation. Rapid development of attack methods requires additional sophisticated protocols to discover novel security threats [4].

Effective prevention-oriented IoT security requires robust attack detection and secure data dissemination to ensure service availability and mitigate risks [5]. In IoT, trust-based interactions are vulnerable to malicious devices that exploit network flaws, which makes robust attack detection crucial, as traditional signature-based methods fail to identify novel threats [6]. Social IoT security is strengthened by ML-driven threat detection and RFID-enabled smart devices, enabling real-time monitoring and seamless interaction between the physical and virtual worlds [7]. Figure 1 illustrates an SIoT architecture. Table I highlights various advanced models for IoT attack detection, including GANs, CNNs, trust management, and hybrid deep learning approaches. Most models achieved improved detection accuracy and adaptability but faced challenges such as overfitting, increased resource consumption, and limited real-time implementation. The main contributions of this study are:

- Develops an effective technique for detecting attacks in SIoT using a hybrid deep learning method, namely Fuzzy Deep Kronecker Stacked Autoencoder (Fuzzy-DKSA), incorporating a Deep Kronecker Network (DKN), a Deep Stacked Autoencoder (DSA), and the fuzzy concept.

- Devises a new technique for feature fusion with a Deep Neural Network (DNN) with a Gower similarity measure to reduce computational complexity.
- Fuzzy logic integration helps manage uncertainty in intrusion detection.

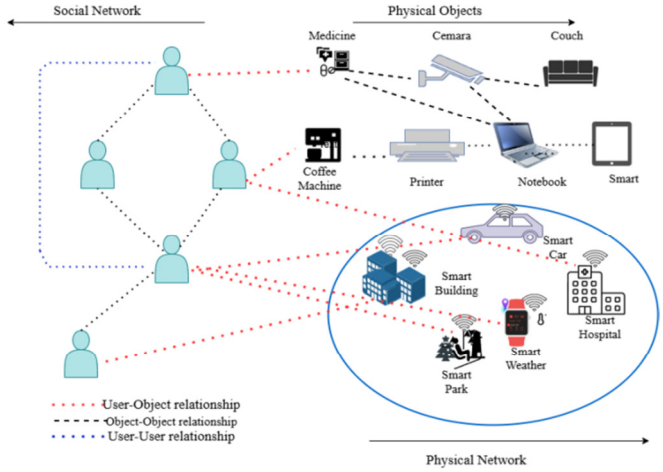

Fig. 1. An SIoT Architecture representing the object and user relationships in the environment.

TABLE I. REVIEW OF RECENT LITERATURE

Ref.	Method/ model used	Key contributions	Limitations
[8]	GAN	Effective in detecting various recent attacks with a reduced false alarm rate	Lacked feature extraction strategies.
[9]	MH-CNN-AM	High prediction rate in detecting deceptive devices	Increased cost due to high adjacent-device communication
[10]	Trust management model	Reduced indecision in selecting dependable suppliers and recognized dynamic actions.	Slightly poorer performance during simple harassment attacks
[11]	ELECTRON mechanism	Achieved elasticity and adaptability for varied deployment environments	Sensitive to attacker behavior changes, reducing performance
[12]	TM-MLA	Identified malicious devices and assigned task-specific trust in real-time	Prone to overfitting and high experimental overhead
[13]	HAD	Ensured trust index-based protection against active/passive attacks	Required high resources and suffered scalability issues at high node densities
[14]	DBN with NMR-LA	Achieved better convergence and lower false positives	Not integrated for synchronized real-time applications
[15]	Distributed deep learning	Prevented local minima during training, excelled in hidden test data scenarios	Ignored data delivery aspects and failed to detect certain critical intrusion patterns

II. PROPOSED METHOD

SIoT data is fed into a data normalization phase that uses Z-score normalization [16] to transform it. The output is then fed into the feature fusion module, which uses a DNN [17] with the Gower similarity measure [18]. The output of the feature fusion module is forwarded to the attack detection module. Here, attack detection is performed using the proposed Fuzzy-DKSA, created by combining DKN [19], DSA [20], and the fuzzy concept. The fuzzy-DKSA for attack detection in SIoT was implemented using MATLAB and the N-BaIoT dataset. Metrics such as precision, F1-score, and accuracy are used to evaluate performance. The efficacy of the proposed model is also contrasted with current techniques. Figure 2 showcases the proposed system architecture for attack detection in SIoT.

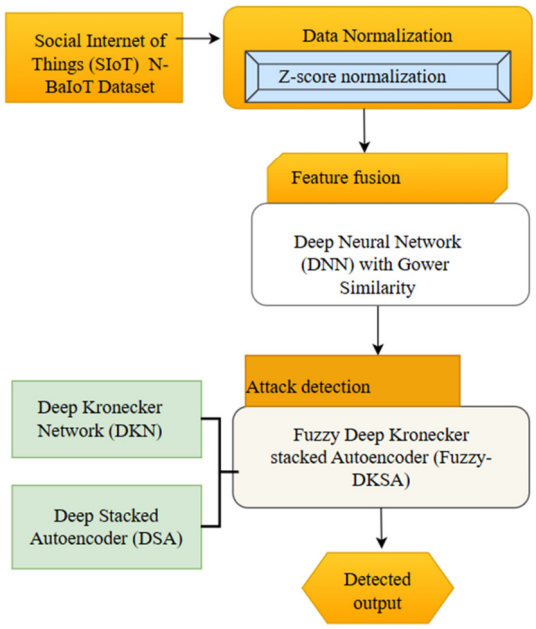

Fig. 2. Proposed system architecture of Fuzzy-DKSA for attack detection in SIoT.

A. *Dataset*

The N-BaIoT dataset [21, 22] contains 7,162,607 samples and 115 features per instance. It was developed to detect IoT-based botnet attacks in realistic conditions. It includes both benign and 10 labeled attack classes executed using the Mirai and Bashlite botnets. Attack types include:

- UDP Flooding
- SYN Flooding
- ACK Flooding
- Scanning
- Host brute force
- OS Scan
- Data Exfiltration
- HTTP Flooding
- TCP Flooding
- Information Theft

```
Algorithm 1: Fuzzy DKSA
Step 1 – Preprocessing:
  Apply Z-score normalization to all 115
  features across  7,162,607  records.
Step 2 – Feature Fusion:
  Use a DNN with Gower similarity to
  integrate features effectively,
  especially those of heterogeneous types.
Step 3 – Detection Using Fuzzy-DKSA:
  DKN captures spatial relationships using
  Kronecker product-based transformations.
  DSA learns compressed feature
  representations and reconstructs them
  for improved anomaly detection.
  Fuzzy Logic Integration: Applies a
  fuzzification function to handle
  imprecision and uncertainty.
Step 4 – Classification
  Final classification is performed using
  a sigmoid layer.
  Binary cross-entropy is
  used as the loss function.
Step 5 – Validation
  The model is evaluated using precision,
  recall, F1-score, and accuracy.
  Comparative results show that the
  proposed model outperforms previous
  state-of-the-art models.
```

The N-BaIoT dataset provides raw input data representing normal and malicious behaviors in SIoT environments. A data point x_i stands for a sample from the dataset, where $i = 1, 2, 3, \dots, N$.

- Let $N = 7{,}162{,}607$ number of samples
- Let $m = 115$ be the number of features per sample.

The dataset contains multiple input features that relate to attack detection. The vector x_i consists of multiple features, which can be written as:

$$x_i = \{f_1, f_2, f_3, \dots, f_{115}\} \quad (1)$$

where f_i stands for the i^{th} feature in the provided dataset. The dataset exists as a matrix because of its structure, which can be expressed through:

$$D = \{x_1, x_2, \dots, x_N\} \in R^{N \times m} \quad (2)$$

Z-score normalization is applied to standardize the input data:

$$X' = \frac{X - \mu}{\sigma} \quad (3)$$

where X' represents the normalized values, X is the primary data point, μ is the mean, and σ is the standard deviation of each feature. This function standardizes feature values to ensure consistent scaling for improved model convergence.

The DNN fuses heterogeneous features using Gower similarity to enhance representation. Normalization makes features measurable on the same scale, which enhances the operational efficiency of deep learning models. DNN and Gower similarity work together to enhance feature representation through their ability to measure mixed-type data similarities.

B. Gower Similarity Calculation

The similarity computation between two vectors x_i and x_j is performed as follows:

$$S_{ij} = \frac{1}{p} \sum_{k=1}^{p} S_{ijk} \quad (4)$$

where S_{ijk} represents the individual feature similarity and p is the total number of features. For numerical features (X_K):

$$S_{ijk} = 1 - \frac{|X_{ik} - X_{jk}|}{R_k} \quad (5)$$

For categorical features (C_K):

$$S_{ijk} = \begin{cases} 1, & if\ x_{ik} = x_{jk} \\ 0, & otherwise \end{cases} \quad (6)$$

The DNN accepts Gower similarity as its input for performing transformations.

$$h_l = f(W_l\, h_{l-1} + b_l) \quad (7)$$

where h_l denotes the activation layer l, W_l and b_l denote layer-specific weights and biases, and $f(\cdot)$ represents the activation function.

DKN utilizes Kronecker products for feature learning:

$$h_l = \sigma(W_l \otimes h_{l-1} + b_l) \quad (8)$$

where $\otimes$ denotes the Kronecker product. DSA follows an encoder-decoder structure, with the encoding layer represented as:

$$h = f\,(W_e X + b_e) \quad (9)$$

and the decoding layer represented as:

$$X' = f\,(W_d h + b_d) \quad (10)$$

where W_e and W_d are the encoder and decoder weight matrices, and b_e and b_d are the bias terms.

C. Fuzzy-DKSA

DKN extracts rich spatial and combinatorial feature interactions using Kronecker product-based transformations. DSA learns compressed representations and reconstructs features to improve anomaly detection sensitivity. Fuzzy-DKSA combines outputs from DKN and DSA with fuzzy logic to handle uncertainty and detect complex attack patterns. This produces the final classification result, identifying whether input traffic is benign or malicious. This is accomplished using a fuzzy membership function:

$$\mu_{A(x)} = \frac{1}{1 + e^{-\beta(x-c)}} \quad (11)$$

where β is the fuzzification parameter and c is the membership center. The decision-making function is:

$$y = \sum_{i=1}^{N} w_i \,.\, \mu_A(x_i) \quad (12)$$

where w_i are weight parameters learned through training. The model classifies the attack using sigmoid activation:

$$\hat{y} = \frac{1}{1+e^{-(w_o h+b_0)}} \quad (13)$$

where W_o and b_o are the output layer weights and bias. Optimization is performed using binary cross-entropy loss:

$$L = -\sum_{i=1}^{n}[y_i\, log(\hat{y}_i) + (1-y_i) log(1-\hat{y}_i)] \quad (14)$$

where y_i represents actual labels, and $\hat{y}_i$ denotes the predicted probability.

- Input stage: Normalized data is passed through the DKN, extracting spatial correlations using Kronecker products for compact and rich feature maps.
- Fuzzy fusion stage: DKN outputs with selected input features are fed into fuzzy nodes to handle uncertainties.
- Encoding-Decoding stage (DSA): The fused output undergoes dimensionality reduction via encoder layers and is reconstructed in the decoder to generate a refined representation for final classification. These components work in tandem to dynamically adapt to diverse SIoT behaviors and attack patterns, improving generalization and trust-aware detection.

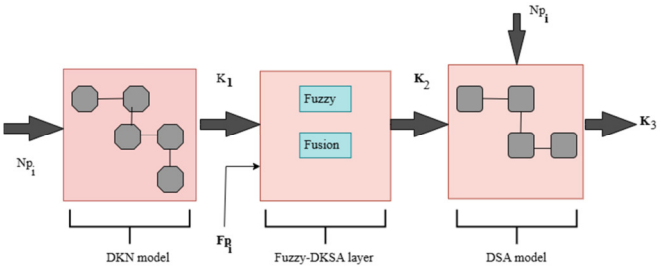

Fig. 3. Design of Fuzzy-DKSA.

III. RESULTS AND DISCUSSIONS

Accuracy, precision, and F1-score were used to evaluate the performance of Fuzzy-DKSA. Figure 4 shows the effectiveness of the Fuzzy-DKSA model in accuracy, achieving 0.915 with 90% training data, surpassing traditional models such as GAN, MH-CNN-AM, TM-MLA, and HAD, which scored 0.88, 0.879, 0889, and 0.89, respectively, resulting in performance improvements of 3.83%, 3.93%,2.84% and 2.73%. In terms of F1-score, Fuzzy-DKSA reached 0.915, while earlier models achieved scores of 0.88, 0.879, 0.889, and 0.890, leading to performance gains of 2.24%, 4.60%, 2.86%, and 2.51%. The Fuzzy-DKSA model demonstrates superior performance across all evaluated metrics, highlighting its effectiveness in attack detection within SIoT networks. Figure 5 demonstrates the performance of the Fuzzy-DKSA model using nine-fold validation, which achieved an accuracy of 0.909, outperforming GAN, MH-CNN-AM, TM-MLA, and HAD, which recorded accuracies of 0.849, 0.86, 0.87, and 0.881, resulting in performance improvements of 6.06%, 5.44%, 4.34% and 3.07%, respectively. Table II shows a comparison of Fuzzy-DKSA with GAN, MH-CNN-AM, TM-MLA, and HAD.

TABLE II. PERFORMANCE OF FUZZY-DKSA

	Metrics	GAN	MH-CNN-AM	TM-MLA	HAD	Proposed Fuzzy-DKSA
Training data	Accuracy	88%	88%	89%	89%	92%
	F1-score	89%	86%	88%	88%	91%
	Precision	86%	88%	87%	87%	91%
Nine-fold cross-validation	Accuracy	85%	86%	87%	88%	91%
	F1-score	86%	87%	87%	88%	91%
	Precision	86%	88%	87%	87%	91%

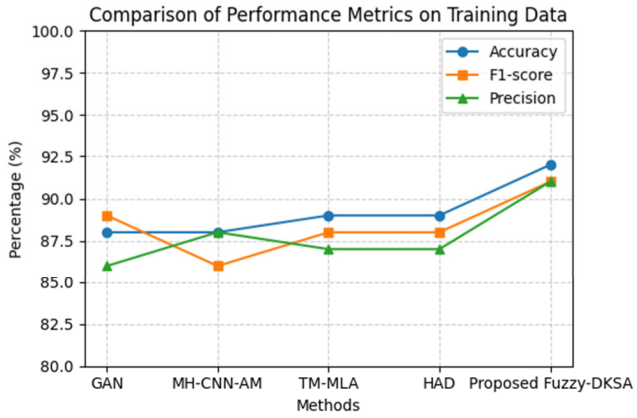

Fig. 4. Comparative evaluation of Fuzzy-DKSA for accuracy, F1-score, and precision.

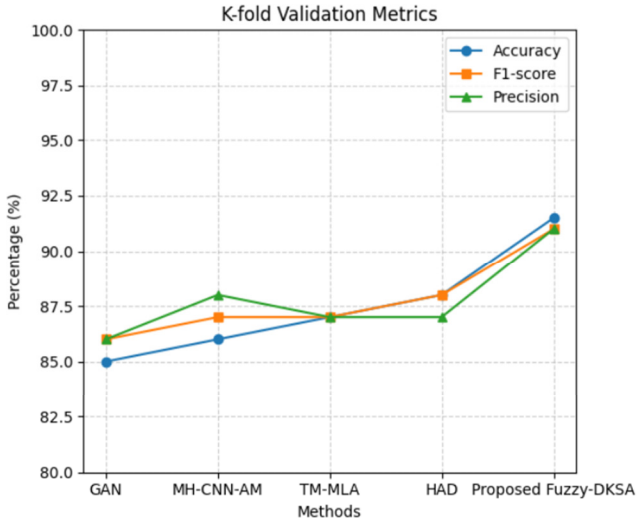

Fig. 5. Comparative analysis of Fuzzy-DKSA based on nine-fold cross-validation.

Table III shows the statistical significance of Fuzzy-DKSA improvement over the baseline models. All p-values were less than 0.05, indicating statistically significant improvements.

TABLE III. STATISTICAL SIGNIFICANCE OF FUZZY-DKSA IMPROVEMENTS OVER BASELINE MODELS

Compared with	Metric	Fuzzy-DKSA Δ (%)	p-value
GAN	Accuracy	+4.0	0.003
MH-CNN-AM	F1-Score	+5.0	0.008
TM-MLA	Precision	+4.0	0.011
HAD	Accuracy	+3.0	0.018

To evaluate the individual contribution of each component in Fuzzy-DKSA, an ablation study was carried out by systematically removing key modules, DKN, DSA, and fuzzy logic, and observing the impact on performance. The results showed that the removal of fuzzy logic significantly reduced precision, while the exclusion of DKN or DSA decreased accuracy and F1-score. The complete model consistently outperformed all reduced configurations, confirming that each component significantly enhances the detection capability.

IV. CONCLUSION

This work presented Fuzzy-DKSA, a novel hybrid model combining DKN, DSA, and fuzzy logic for effective attack detection in SIoT. The integration of Gower similarity enables efficient fusion of heterogeneous features. The model is designed to handle the uncertainty and dynamic relationships inherent in SIoT environments. Unlike conventional methods, it offers enhanced adaptability and trust-aware decision-making. The experimental results demonstrate superior accuracy, precision, and F1-score compared to existing techniques. Future research will extend this work by exploring more advanced deep learning architectures, such as transformer-based models and graph neural networks, to further improve detection capabilities. In addition, real-time deployment in diverse SIoT environments will be investigated to address issues related to scalability, computational efficiency, and dynamic network behavior. Incorporating adaptive fuzzy systems and continual learning strategies will also be considered to enhance the model's adaptability to evolving cyber threats.

The integration of DKN, DSA, and fuzzy logic increases computational overhead and may require careful parameter tuning. Scalability and real-time performance could be affected in resource-constrained or high-density IoT environments. Despite its layered complexity, the Fuzzy-DKSA model is modular and can be optimized using pruning or quantization techniques. This enables practical deployment on cloud or edge platforms with manageable training time and resource consumption.

REFERENCES

[1] R. Latif, "ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things," *IEEE Access*, vol. 10, pp. 46526–46537, 2022, https://doi.org/10.1109/ACCESS.2022.3169788.

[2] S. Divya, R. Tanuja, S. H. Manjula, and K. R. Venugopal, "Securing Social Internet of Things: Intrusion Detection Models in Collaborative Edge Computing," in *Proceedings of 4th International Conference on Frontiers in Computing and Systems*, 2024, pp. 103–113, https://doi.org/10.1007/978-981-97-2614-1_8.

[3] S. Divya and R. Tanuja, "Enhancing SIoT Security Through Advanced Machine Learning Techniques for Intrusion Detection," in *Communication and Intelligent Systems*, 2024, pp. 105–116, https://doi.org/10.1007/978-981-97-2053-8_8.

[4] M. Rahouti, M. Ayyash, S. K. Jagatheesaperumal, and D. Oliveira, "Incremental Learning Implementations and Vision for Cyber Risk Detection in IoT," *IEEE Internet of Things Magazine*, vol. 4, no. 3, pp. 114–119, Sep. 2021, https://doi.org/10.1109/IOTM.0011.2100019.

[5] M. A. Alqarni and S. H. Chauhdary, "A Security Scheme for Statistical Anomaly Detection and the Mitigation of Rank Attacks in RPL Networks (IoT Environment)," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12409–12414, Dec. 2023, https://doi.org/10.48084/etasr.6433.

[6] T. Al-Shurbaji *et al.*, "Deep Learning-Based Intrusion Detection System for Detecting IoT Botnet Attacks: A Review," *IEEE Access*, vol. 13, pp. 11792–11822, 2025, https://doi.org/10.1109/ACCESS.2025.3526711.

[7] R. M.s., S. Pattar, R. Buyya, V. K.r., S. S. Iyengar, and L. M. Patnaik, "Social Internet of Things (SIoT): Foundations, thrust areas, systematic review and future directions," *Computer Communications*, vol. 139, pp. 32–57, May 2019, https://doi.org/10.1016/j.comcom.2019.03.009.

[8] L. Nie *et al.*, "Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 134–145, Oct. 2022, https://doi.org/10.1109/TCSS.2021.3063538.

[9] R. M. Das *et al.*, "A novel deep learning-based approach for detecting attacks in social IoT," *Soft Computing*, May 2023, https://doi.org/10.1007/s00500-023-08389-1.

[10] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 3297–3308, Sep. 2021, https://doi.org/10.1109/TNSM.2020.3046906.

[11] G. H. C. de Oliveira, A. de Souza Batista, M. Nogueira, and A. L. dos Santos, "An access control for IoT based on network community perception and social trust against Sybil attacks," *International Journal of Network Management*, vol. 32, no. 1, 2022, Art. no. e2181, https://doi.org/10.1002/nem.2181.

[12] P. Hankare, S. Babar, and P. Mahalle, "Trust Management Approach for Detection of Malicious Devices in SIoT," *Tehnički glasnik*, vol. 15, no. 1, pp. 43–50, Mar. 2021, https://doi.org/10.31803/tg-20210204180217.

[13] M. S. Mekala, G. Srivastava, J. H. Park, and H. Y. Jung, "An effective communication and computation model based on a hybridgraph-deeplearning approach for SIoT," *Digital Communications and Networks*, vol. 8, no. 6, pp. 900–910, Dec. 2022, https://doi.org/10.1016/j.dcan.2022.07.004.

[14] M. Ramesh Babu and K. N. Veena, "Optimal DBN-based distributed attack detection model for Internet of Things," *International Journal of Communication Systems*, vol. 33, no. 17, 2020, Art. no. e4595, https://doi.org/10.1002/dac.4595.

[15] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Generation Computer Systems*, vol. 82, pp. 761–768, May 2018, https://doi.org/10.1016/j.future.2017.08.043.

[16] M. Z. Al-Faiz, A. A. Ibrahim, and S. M. Hadi, "The effect of Z-Score standardization (normalization) on binary input due the speed of learning in back-propagation neural network," *Iraqi Journal of Information and Communication Technology*, vol. 1, no. 3, pp. 42–48, 2018.

[17] H. Mohsen, E. S. A. El-Dahshan, E. S. M. El-Horbaty, and A. B. M. Salem, "Classification using deep learning neural networks for brain tumors," *Future Computing and Informatics Journal*, vol. 3, no. 1, pp. 68–71, Jun. 2018, https://doi.org/10.1016/j.fcij.2017.12.001.

[18] S. H. Cha, "Comprehensive Survey on Distance/Similarity Measures between Probability Density Functions," *International Journal of Mathematical models and Methods in Applied Sciences*, vol. 1, no. 4, pp. 300–307, 2007.

[19] L. Feng and G. Yang, "Deep Kronecker network," *Biometrika*, vol. 111, no. 2, pp. 707–714, Jun. 2024, https://doi.org/10.1093/biomet/asad049.

[20] A. Dairi, F. Harrou, Y. Sun, and M. Senouci, "Obstacle Detection for Intelligent Transportation Systems Using Deep Stacked Autoencoder and k-Nearest Neighbor Scheme," *IEEE Sensors Journal*, vol. 18, no. 12, pp. 5122–5132, Jun. 2018, https://doi.org/10.1109/JSEN.2018.2831082.

[21] Y. Meidan *et al.*, "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, Apr. 2018, https://doi.org/10.1109/MPRV.2018.03367731.

[22] "N-BaIoT Dataset to Detect IoT Botnet Attacks." Kaggle, [Online]. Available: https://www.kaggle.com/datasets/mkashifn/nbaiot-dataset.