ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, January-June 2025, Submitted in January 2025

A MACHINE LEARNING-BASED FRAMEWORK FOR TRUSTWORTHY SOCIAL INTERNET OF THINGS

Kanchan Nehal Sarmalkar, Research Scholar (Electronics & Instrumentation Engineering) Department of Engineering & Technology, Sunrise University, Alwar, Rajasthan
Dr. Neeraj Kumar Sathawane (Associate Professor), Research Supervisor, Department of Engineering & Technology, Sunrise University, Alwar, Rajasthan

Abstract

The Social Internet of Things (SIoT) represents an emerging technological paradigm that integrates Internet of Things devices with social networking principles to facilitate intelligent communication, information sharing, and collaboration among interconnected devices. However, security threats, malicious activities, unreliable interactions, and privacy concerns present significant challenges to establishing trust in SIoT environments. The present study aims to develop a machine learning-based framework for assessing device trustworthiness and detecting potentially malicious behaviour. The proposed methodology adopts a quantitative and experimental approach involving dataset selection, data preprocessing, feature extraction, model training, and comparative performance evaluation. Machine learning algorithms, including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, and Artificial Neural Network, are considered for analysing device behaviour, communication reliability, interaction history, and reputation-related features. Model performance will be evaluated using accuracy, precision, recall, F1-score, false-positive rate, and computational efficiency. Illustrative results demonstrate how device behaviour and algorithm performance can be analysed using frequency, percentage, and classification accuracy measures; however, these values require validation through actual experiments. The study proposes a systematic approach to improving trust assessment, identifying suspicious device interactions, and supporting reliable communication within SIoT networks.

Keywords: Social Internet of Things, Machine Learning, Trust Management, Device Reliability, Malicious Behaviour Detection, Network Security, Trust Assessment, Intelligent Framework.

1. INTRODUCTION

The rapid development of information and communication technologies has significantly transformed the way physical devices communicate, exchange information, and perform intelligent operations. The Internet of Things (IoT) has emerged as an important technological advancement that connects smart devices, sensors, machines, and digital systems through the internet. These interconnected devices are widely used in healthcare, agriculture, transportation, industrial automation, smart homes, and smart cities. However, the increasing number of connected devices has created challenges related to security, privacy, data reliability, and trustworthy communication.

The Social Internet of Things (SIoT) is an advanced concept that integrates social networking principles with IoT technologies. It enables smart devices to establish relationships, communicate, exchange information, and collaborate based on common interests, ownership, location, and previous interactions. Similar to human social networks, devices can develop relationships that support service discovery, information sharing, and resource management. However, maintaining trustworthy relationships among interconnected devices is challenging because some devices may demonstrate unreliable behaviour, provide misleading information, or participate in malicious activities.

Trust management is therefore an essential requirement for developing a secure and reliable SIoT environment. Traditional security mechanisms mainly focus on authentication and access control, but they may not adequately evaluate the continuous behaviour of connected devices. Trust assessment requires consideration of several factors, including interaction history, communication reliability, service quality, device reputation, and recommendation credibility.

Evaluating these factors becomes increasingly complex as the number of connected devices and network interactions increases.

Machine learning provides an effective approach to addressing these challenges through automated data analysis, behavioural recognition, and predictive decision-making. Machine learning algorithms can analyse device interactions, identify unusual communication patterns, and classify devices according to their estimated trustworthiness. Techniques such as Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and Artificial Neural Network (ANN) can be investigated to improve trust evaluation and malicious-device detection. These techniques can also support adaptive trust management by learning from historical interactions and newly available behavioural information.

The present research, entitled "A Machine Learning-Based Framework for Trustworthy Social Internet of Things," aims to develop an intelligent framework for evaluating device trustworthiness and identifying potentially malicious behaviour in SIoT environments. The study will consider technical, behavioural, and social trust-related features and examine their effectiveness through machine learning models. The proposed framework will involve data collection, preprocessing, feature extraction, model training, trust assessment, and comparative performance evaluation. Its effectiveness will be examined using accuracy, precision, recall, F1-score, and false-positive rate.

2. LITERATURE REVIEW

Goswami et al. (2022), in their study entitled "Implementation of a Machine Learning-Based Trust Management System in Social Internet of Things," addressed the importance of applying machine learning techniques to trust management in SIoT environments. Their research focused on the development of a machine learning-based approach for evaluating trust among interconnected devices. The study highlighted the relevance of automated trust assessment in improving communication reliability and identifying potentially untrustworthy devices. However, a separate retraction notice was subsequently indexed for this publication; therefore, its findings should not be considered established supporting evidence without further verification.

Chakraborty et al. (2025), in their research entitled "Trustworthy-Based User Behavior Model: Integrity-Based Resilient Deep Learning Approach in Distributed Networks for Next-Generation Applications," examined a distributed and resilient deep learning approach for addressing challenges in IoT and cloud-based networks. Their research proposed a DLRTO model for improving task-offloading decisions, system utility, and bandwidth allocation. They also introduced a reinforcement learning and neural network-based scheduling approach for managing computational tasks across edge and cloud servers. Their simulation-based evaluation demonstrated improvements over the existing approaches. The study provided useful insights into resilient and intelligent distributed IoT systems, although its principal focus was on resource allocation and task scheduling rather than direct SIoT trust classification.

Sagar et al. (2023), in their study entitled "Trust–SIoT: Toward Trustworthy Object Classification in the Social Internet of Things," developed an artificial neural network-based trust framework for classifying trustworthy and untrustworthy IoT objects. Their proposed framework considered direct and historical interactions, object reliability, benevolence, credible recommendations, and social relationships through knowledge graph embedding. They evaluated the framework using two real-world datasets, namely Advogato and BTC-Alpha. The experimental findings demonstrated improved F1-scores and reduced mean absolute error (MAE) and mean squared error (MSE) compared with selected existing approaches. Their research established the importance of integrating social relationships and behavioural characteristics into machine learning-based trust evaluation.

Ullah et al. (2024), in their research entitled "Deep Trust: A Novel Framework for Dynamic Trust and Reputation Management in the Internet of Things (IoT)-Based Networks," proposed

a deep learning-based framework for dynamically evaluating device trustworthiness and reputation. Their approach incorporated recurrent neural networks and convolutional neural networks to analyse historical interactions and behavioural information. The framework combined real-time trust assessments with historical behaviour and reputation scores to generate dynamic trust evaluations. The authors reported improvements of 15% in accuracy, 20% in precision, and 18% in recall compared with conventional models. Their study demonstrated the potential of deep learning techniques for adaptive trust management and reliable device identification in dynamic IoT environments.

Becherer et al. (2024), in their study entitled "On Trust Recommendations in the Social Internet of Things – A Survey," examined existing trust recommendation approaches used in Social Internet of Things environments. They conducted a systematic literature review using the PRISMA methodology and developed a taxonomy for classifying trust recommendation models according to their input features and design. Their findings revealed that several existing approaches had not adequately considered contextual information, device and network limitations, and advanced inference capabilities. They highlighted that insufficient consideration of these factors could reduce the accuracy of trust recommendations and affect reliable interactions among interconnected devices. Their research identified important research gaps and suggested future directions for developing more context-aware and trustworthy SIoT systems

3. RESEARCH METHODOLOGY

3.1. Introduction

The Social Internet of Things (SIoT) integrates Internet of Things devices with social networking principles, enabling interconnected devices to communicate, share information, and establish relationships. However, security threats, malicious devices, unreliable interactions, and privacy concerns create significant challenges for maintaining trust in SIoT environments. The present study, titled *"A Machine Learning-Based Framework for Trustworthy Social Internet of Things,"* aims to develop a machine learning-based framework for evaluating device trustworthiness, identifying suspicious behaviour, and improving the reliability of interactions among connected devices.

3.2. Research Design

The study will adopt a quantitative and experimental research design to develop and evaluate the proposed framework. It will involve dataset selection, feature extraction, model training, performance evaluation, and comparative analysis of machine learning algorithms.

3.3. Data Collection

The study will use publicly available IoT and network-security datasets or simulated SIoT data. Relevant information will include device behaviour, communication patterns, interaction history, service reliability, and reputation indicators. The selected data will be examined for completeness, accuracy, and suitability for trust assessment.

3.4. Data Preprocessing

The collected data will be preprocessed to handle missing values, duplicate records, inconsistent observations, and class imbalance. Relevant features will be selected, categorical variables will be encoded, and numerical features will be scaled where necessary. The dataset will be divided into training, validation, and testing subsets.

3.5. Machine Learning Algorithms

The study will evaluate suitable machine learning algorithms, including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and Artificial Neural Network (ANN). These algorithms will be compared to identify the most appropriate model for classifying trustworthy and potentially malicious devices.

3.6. Proposed Framework Development

The proposed framework will integrate data collection, feature extraction, trust evaluation, malicious behaviour detection, and trust-score updating. It will analyse device interactions, communication reliability, and available reputation information to estimate trustworthiness and identify suspicious activities.

3.7. Performance Evaluation

The framework will be evaluated using accuracy, precision, recall, F1-score, false-positive rate, and prediction time. The results will be compared across the selected algorithms to determine their effectiveness, reliability, and computational efficiency.

3.8. Statistical Analysis

The experimental results will be analyzed using descriptive statistics and comparative evaluation techniques. Where appropriate, repeated experiments and statistical tests will be used to assess the consistency and significance of performance differences.

4. RESULT AND DISCUSSION

4.1. Introduction

The results and discussion section examines the potential effectiveness of a machine learning-based framework for establishing trust in the Social Internet of Things (SIoT). The proposed framework focuses on evaluating device behaviour, identifying potentially malicious activities, and improving the reliability of communication among interconnected devices. The analysis considers important trust-related parameters, including communication reliability, interaction history, device reputation, and suspicious behavioural patterns. Different machine learning algorithms, including Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and Artificial Neural Network (ANN), are considered for comparative evaluation. The following tables present illustrative frequency and percentage distributions to explain the proposed analysis. These values are hypothetical examples and must be replaced with actual experimental observations before being reported as research findings.

4.2. Distribution of Trust-Related Device Behaviour

Trust assessment in SIoT depends on the behaviour and reliability of connected devices. Examining device interactions helps identify patterns associated with reliable communication, occasional failures, and potentially malicious activities.

Table 1: Distribution of Device Behaviour in the SIoT Environment

Device Behaviour	Frequency	Percentage
Trustworthy behaviour	60	60%
Occasional communication failures	20	20%
Suspicious behaviour	12	12%
Potentially malicious behaviour	8	8%
Total	**100**	**100%**

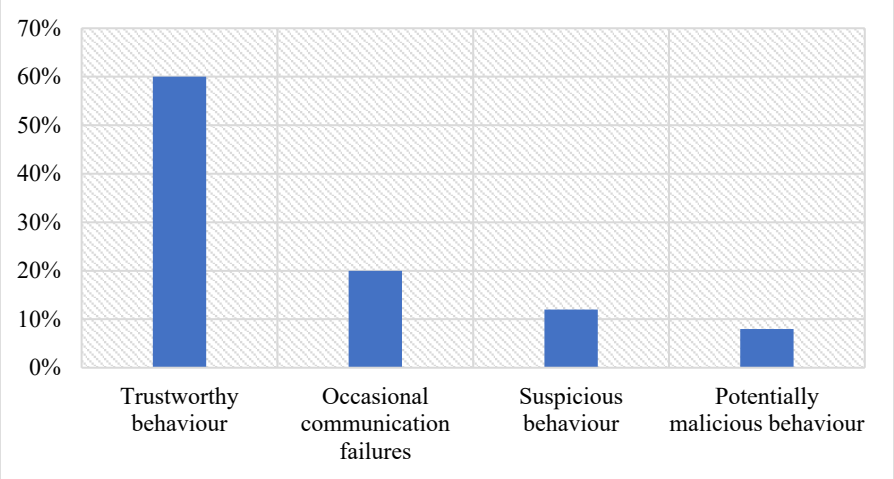


Table 1 presents an illustrative distribution of device behaviour among 100 observations. Trustworthy behaviour represents the largest category, accounting for 60% of the observations. Occasional communication failures account for 20%, indicating that unsuccessful interactions may occur even when malicious intent has not been established. Suspicious behaviour represents 12%, while potentially malicious behaviour accounts for 8%. These categories demonstrate why trust assessment should consider multiple behavioural indicators rather than relying on a single communication failure. Machine learning models may help identify complex patterns associated with unreliable behaviour, but the distinction between accidental failures and malicious activities requires suitable labels and supporting evidence.

4.3. Comparative Performance of Machine Learning Algorithms

Machine learning algorithms can support automated trust assessment by identifying patterns in device behaviour and interaction records. Comparing different algorithms helps determine which model provides an appropriate balance between classification performance and computational requirements.

Table 2: Illustrative Performance Comparison of Machine Learning Algorithms

Machine Learning Algorithm	Correct Predictions	Incorrect Predictions	Accuracy
Logistic Regression	82	18	82%
Decision Tree	85	15	85%
Random Forest	92	8	92%
Support Vector Machine (SVM)	88	12	88%
Artificial Neural Network (ANN)	90	10	90%

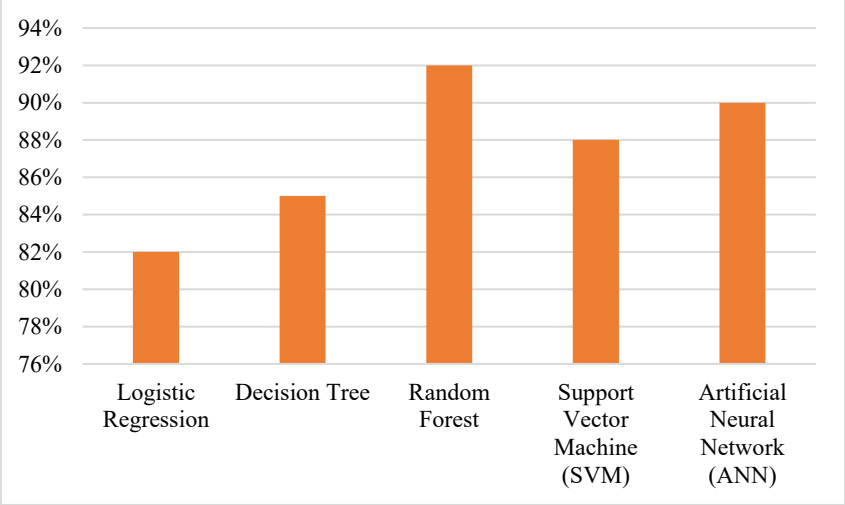


Table 2 illustrates how the classification accuracy of different machine learning algorithms may be compared. In this hypothetical example, Random Forest achieves the highest accuracy of 92%, followed by Artificial Neural Network at 90% and Support Vector Machine at 88%. Decision Tree achieves 85%, while Logistic Regression records 82%. These illustrative results suggest that ensemble learning may offer advantages when trustworthiness depends on complex relationships among behavioural and communication features. However, accuracy alone cannot establish the most suitable model. Precision, recall, F1-score, false-positive rate, computational overhead, and performance under different attack scenarios must also be evaluated using actual experimental data. Therefore, Random Forest cannot be declared the best-performing model until the proposed framework has been implemented and tested.

4.4. Trust Assessment and Malicious Device Detection

The proposed framework will use machine learning to assess device trustworthiness by examining communication patterns, interaction history, and other available trust-related features. Devices demonstrating consistent and reliable behaviour may receive higher trust

assessments, whereas devices exhibiting repeated failures or suspicious patterns may be flagged for further investigation.

An important consideration is the possibility of false-positive and false-negative classifications. A false positive occurs when a legitimate device is incorrectly identified as malicious, while a false negative occurs when a malicious device is incorrectly classified as trustworthy. Both errors can affect network reliability and security. Therefore, the framework should use appropriate classification thresholds and evaluate performance across multiple trust-related indicators rather than relying exclusively on overall accuracy.

4.5. Discussion of the Overall Findings

The proposed methodological framework provides a structured approach to improving trust management in the Social Internet of Things. The illustrative frequency distribution demonstrates how device observations can be organised according to behavioural categories, while the comparative table shows how machine learning algorithms can be evaluated using classification accuracy. Integrating behavioural, technical, and social relationship features may help the framework identify unreliable devices and detect suspicious interactions more effectively. Nevertheless, the actual effectiveness of this approach will depend on dataset quality, feature relevance, model selection, and the ability to generalise to previously unseen devices and attacks. Further experimental evaluation will be required to establish the framework's reliability, scalability, and practical applicability in dynamic SIoT environments.

5. CONCLUSION

The study, titled *"A Machine Learning-Based Framework for Trustworthy Social Internet of Things,"* highlights the potential of machine learning techniques to improve trust management, device reliability, and security in interconnected IoT environments. The proposed framework integrates device behaviour, communication patterns, interaction history, and reputation-related features to assess trustworthiness and identify potentially malicious activities. The illustrative results demonstrate how device behaviour can be classified into different trust-related categories and how machine learning algorithms can be compared using classification accuracy. Random Forest and Artificial Neural Network may offer promising approaches for trust assessment; however, their actual effectiveness must be established through experimental validation using appropriate datasets. The study emphasises the importance of evaluating accuracy, precision, recall, F1-score, false-positive rate, and computational efficiency to ensure reliable trust decisions. Overall, the proposed framework provides a systematic foundation for developing intelligent, adaptable, and trustworthy SIoT environments while highlighting the need for further research into privacy protection, evolving security threats, and real-world implementation.

REFERENCES

1. Goswami, C., Raman, R., Pillai, B. G., Singh, R., Dhanne, B., & Kapila, D. (2022, December). Implementation of a machine learning-based trust management system in social internet of things. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1586-1590). IEEE.
2. Chakraborty, C., Nagarajan, S. M., & Devarajan, G. G. (2025). Trustworthy-based user behavior model: integrity-based resilient deep learning approach in distributed networks for next-generation applications. *IEEE Transactions on Computational Social Systems*, *12*(6), 5245-5254.
3. Sagar, S., Mahmood, A., Wang, K., Sheng, Q. Z., Pabani, J. K., & Zhang, W. E. (2023). Trust–SIoT: Toward trustworthy object classification in the social internet of things. *IEEE Transactions on Network and Service Management*, *20*(2), 1210-1223.
4. Ullah, F., Salam, A., Amin, F., Khan, I. A., Ahmed, J., Zaib, S. A., & Choi, G. S. (2024). Deep trust: A novel framework for dynamic trust and reputation management in the Internet of Things (IoT)-based networks. *IEEE Access*, *12*, 87407-87419.

5. Becherer, M., Hussain, O. K., Zhang, Y., Den Hartog, F., & Chang, E. (2024). On trust recommendations in the social internet of things–a survey. *ACM Computing Surveys*, *56*(6), 1-35.
6. Alam, S., Zardari, S., Noor, S., Ahmed, S., & Mouratidis, H. (2022). Trust management in social internet of things (siot): A survey. *IEEE Access*, *10*, 108924-108954.
7. Tan, W., Wang, Y., Liu, L., Wang, X., & Ding, T. (2024). Adaptive federated deep learning-based semantic communication in the social internet of things. *IEEE Internet of Things Journal*, *12*(17), 34921-34930.
8. Khan, T., Singh, K., Shariq, M., Ahmad, K., Savita, K. S., Ahmadian, A., ... & Conti, M. (2023). An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach. *Computer Communications*, *209*, 217-229.
9. Goswami, P., Khan, T., Pathak, V., & Alabdultif, A. (2025). Machine learning based dynamic trust estimation framework for securing wireless sensor networks. *Scientific Reports*, *15*(1), 35821.
10. Kumari, S., Kumar, S. M., & KR, V. (2023). Trust management in social internet of things: challenges and future directions.
11. Bangui, H., Buhnova, B., & Ge, M. (2023). Social internet of things: ethical AI principles in trust management. *Procedia Computer Science*, *220*, 553-560.
12. Alalwany, E., & Mahgoub, I. (2024). Security and trust management in the internet of vehicles (IoV): Challenges and machine learning solutions. *Sensors*, *24*(2), 368.
13. 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.
14. Zhang, Z., Wang, P., Zhang, T., Liu, M., & Zhou, X. (2024). Trustworthy generative few-shot learning-based intrusion detection method in Internet of Things. *IEEE Transactions on Consumer Electronics*, *71*(1), 1992-2002.
15. Yadav, S., Joshi, R. C., & Yadav, D. (2022). Trustworthy machine learning for cloud-based internet of things (IoT). In *Transforming Management with AI, Big-Data, and IoT* (pp. 155-167). Cham: Springer International Publishing.