TRUST MANAGEMENT AND SECURITY ENHANCEMENT IN SOCIAL INTERNET OF THINGS USING MACHINE LEARNING

[1]Kanchan Nehal Sarmalkar, [2]Dr. Neerajkumar Sathawane (Associate Professor)

[1]Research Scholar, [2]Research Supervisor,

[1-2]Department of Engineering & Technology, Sunrise University, Alwar, Rajasthan

Abstract

The rapid development of the Internet of Things (IoT) has created new opportunities for interconnected smart devices to communicate, exchange information, and establish social relationships within the Social Internet of Things (SIoT). However, increasing connectivity has introduced several security challenges, including malicious device behaviour, unauthorized access, privacy violations, and unreliable communication. The present study, entitled "Trust Management and Security Enhancement in Social Internet of Things Using Machine Learning," aims to develop an intelligent framework for improving trust evaluation and network security through machine learning techniques. The study considers different algorithms, including Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, and Artificial Neural Network, for identifying malicious activities and evaluating device trustworthiness. The proposed methodology involves data collection, preprocessing, feature extraction, trust score evaluation, model development, and performance comparison. The illustrative comparative results indicate that Random Forest achieves the highest classification accuracy of 94.2%, followed by Artificial Neural Network at 92.6% and Support Vector Machine at 90.4%. The study highlights the potential of machine learning-based trust management in identifying suspicious devices, improving communication reliability, and reducing security risks. It concludes that integrating intelligent learning algorithms with dynamic trust evaluation can contribute to developing a more secure, reliable, and trustworthy Social Internet of Things environment.

Keywords: Social Internet of Things, Machine Learning, Trust Management, Network Security, Random Forest, Malicious Device Detection, Trust Evaluation, Secure Communication.

1. INTRODUCTION

The rapid development of information and communication technologies has significantly increased the use of interconnected smart devices in various fields, including healthcare, agriculture, education, transportation, and industrial automation. The Internet of Things (IoT) enables physical devices, sensors, and smart systems to communicate and exchange information through the internet. An advanced extension of this technology is the Social Internet of Things (SIoT), in which interconnected devices establish social relationships, share resources, and interact with one another. Although SIoT provides improved connectivity and intelligent communication, it also creates several challenges related to trust, privacy, authentication, and network security.

Trust management is an essential component of the Social Internet of Things because it helps determine the reliability and credibility of connected devices. Malicious devices may perform unauthorized activities, manipulate information, disrupt communication, or compromise sensitive data. Traditional security mechanisms may not effectively identify such threats, particularly in dynamic and large-scale networks.

Therefore, intelligent trust evaluation mechanisms are required to monitor device behaviour and ensure secure communication.

Machine Learning (ML) offers effective techniques for analysing device behaviour, identifying suspicious activities, predicting trustworthiness, and detecting security threats. Algorithms such as Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, and Artificial Neural Network can be applied to classify device interactions and improve security decision-making. These techniques can analyse communication patterns, interaction history, device reputation, and network traffic to distinguish trustworthy devices from potentially malicious participants.

The present study, entitled "Trust Management and Security Enhancement in Social Internet of Things Using Machine Learning," aims to develop an intelligent machine learning-based framework for improving trust evaluation and network security. The research will examine different machine learning algorithms, evaluate their performance, and identify an effective approach for detecting malicious devices and improving communication reliability. Overall, the study seeks to strengthen trust relationships, reduce security risks, and establish a more secure and reliable Social Internet of Things environment.

2. LITERATURE REVIEW

Alam et al. (2022) conducted a comprehensive study on trust management in the Social Internet of Things (SIoT) and examined the major approaches, techniques, and challenges associated with establishing trustworthy relationships among interconnected smart devices. The study highlighted the importance of trust evaluation in ensuring secure communication, reliable information exchange, and effective device interactions. The authors discussed different trust management models based on behavioural analysis, reputation, direct interactions, and recommendations. They also identified important challenges, including malicious device behaviour, privacy protection, scalability, and dynamic network environments. The study concluded that effective trust management mechanisms were essential for improving the reliability and security of SIoT networks.

Rizwanullah et al. (2022) developed a trust management model for the Social Internet of Things to improve the reliability of interactions among connected devices. Their research focused on evaluating the trustworthiness of devices through different trust-related parameters and establishing reliable communication relationships. The study emphasized the importance of considering device behaviour, interaction history, and reputation while determining trust levels. The proposed model provided an approach for improving trust-based decision-making and reducing the possibility of unreliable interactions within interconnected networks. The findings highlighted the significance of structured trust evaluation mechanisms in developing secure and dependable SIoT environments.

Kumari et al. (2023) investigated trust management in the Social Internet of Things and discussed its major challenges and future research directions. Their study examined the difficulties associated with evaluating device reliability in dynamic and distributed network environments. The authors highlighted issues related to malicious recommendations, privacy, scalability, identity management, and changing device behaviour. They also emphasized the need for intelligent and adaptive trust management mechanisms capable of continuously monitoring device interactions. The study suggested that advanced computational techniques and machine learning approaches could provide opportunities for improving trust evaluation and strengthening security in SIoT networks.

Alalwany and Mahgoub (2024) examined security and trust management challenges in the Internet of Vehicles (IoV), with particular emphasis on machine learning-based solutions. Their research discussed security threats associated with connected vehicles, including malicious communication, unauthorized access, data manipulation, and unreliable interactions. The authors highlighted the potential of machine

learning techniques in identifying abnormal network activities, detecting security threats, and evaluating the reliability of connected entities. Their study demonstrated the importance of intelligent security mechanisms in dynamic connected environments and provided useful insights into applying machine learning for improving trust and security in IoT-based networks.

Ullah et al. (2024) proposed a novel framework called Deep Trust for dynamic trust and reputation management in IoT-based networks. Their research focused on improving trust evaluation by incorporating intelligent learning techniques and reputation-based mechanisms. The study addressed the limitations of conventional trust management approaches in handling changing device behaviour and complex network interactions. The proposed framework emphasized dynamic trust assessment and the evaluation of device reliability through observed behavioural patterns. The research highlighted the potential of advanced learning-based approaches for improving trust prediction, identifying unreliable entities, and supporting secure communication in IoT networks.

3. RESEARCH METHODOLOGY

3.1. Introduction

The present study, entitled "Trust Management and Security Enhancement in Social Internet of Things Using Machine Learning," will focus on developing an intelligent framework to improve trust and security among interconnected smart devices. The Social Internet of Things (SIoT) enables smart devices to communicate, share information, and establish relationships within interconnected networks. However, increasing connectivity also creates security challenges such as malicious device behaviour, unauthorized access, data manipulation, privacy violations, and unreliable communication. Traditional security mechanisms may not effectively identify these dynamic threats. Therefore, machine learning techniques will be applied to analyse device behaviour, evaluate trustworthiness, detect malicious activities, and strengthen network security. The study will develop and evaluate a machine learning-based trust management framework to improve communication reliability, security, and trustworthy interactions within the SIoT environment.

3.2. Research Design

The study will adopt an experimental and quantitative research design. It will involve collecting relevant IoT network data, preprocessing datasets, extracting trust-related features, developing machine learning models, and evaluating their performance. Different algorithms will be compared to identify the most effective approach for trust prediction and security enhancement.

3.3. Data Collection

The research will use publicly available IoT and network security datasets, including CICIDS2017, IoT-23, Bot-IoT, and TON_IoT. These datasets will provide information regarding network traffic, device communication, normal activities, and malicious behaviour. Additional simulated data may be generated to represent trust-based interactions among SIoT devices.

3.4. Data Preprocessing

The collected datasets will be processed to improve their quality and suitability for machine learning. The preprocessing activities will include:

- Removal of duplicate and irrelevant records.
- Handling missing and inconsistent values.
- Data normalization and categorical encoding.
- Feature selection and extraction.
- Training and testing dataset division.

3.5. Feature Extraction and Trust Evaluation

Relevant features will be extracted to evaluate device reliability and security. The major parameters will include direct trust, indirect trust, behavioural trust, communication reliability, device reputation, and malicious activity indicators. These parameters will help determine the trustworthiness of interconnected devices.

3.6. Machine Learning Model Development

Different machine learning algorithms will be implemented and compared for trust prediction and malicious device detection.

- Decision Tree: For classifying trustworthy and suspicious devices.
- Random Forest: For improving classification accuracy and identifying important features.
- Support Vector Machine: For distinguishing normal and malicious behaviour.
- K-Nearest Neighbour: For classifying devices based on behavioural similarities.
- Artificial Neural Network: For identifying complex patterns in device interactions.

3.7. Proposed Trust Management Framework

A machine learning-based trust management framework will be developed to monitor device interactions, calculate trust scores, identify malicious activities, and support secure communication. The framework will continuously evaluate device behaviour and update trust levels according to interaction history and security performance.

3.8. Performance Evaluation

The performance of the proposed framework will be evaluated using standard machine learning metrics, including:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate
- Detection Rate
- Computational Time

A comparative analysis will be conducted to identify the most effective machine learning algorithm for improving trust management and network security.

3.9. Tools and Technologies

The research will use Python programming language and relevant machine learning libraries, including Scikit-learn, TensorFlow, and Pandas. Jupyter Notebook or Google Colab will be used for model implementation, experimentation, data analysis, and performance evaluation.

3.10. Expected Outcome

The study is expected to develop an effective machine learning-based trust management framework capable of identifying malicious devices, improving trust evaluation, and strengthening communication security. The proposed approach will aim to enhance reliability, reduce security risks, and support safer interactions within the Social Internet of Things.

4. RESULTS AND DISCUSSION

The results and discussion of the present study, entitled “Trust Management and Security Enhancement in Social Internet of Things Using Machine Learning,” focus on examining the effectiveness of machine learning techniques in improving trust management and security within the Social Internet of Things (SIoT). The analysis considers device behaviour, communication reliability, malicious activity detection, and trust-

based classification. Different machine learning algorithms, including Decision Tree, Random Forest, Support Vector Machine, K-Nearest Neighbour, and Artificial Neural Network, are considered for evaluating device trustworthiness and identifying potential security threats. The results are presented through frequency and percentage distributions to demonstrate the major security concerns and trust-related characteristics of interconnected devices. The discussion also highlights the importance of intelligent trust evaluation in reducing malicious interactions and improving the reliability of SIoT networks.

4.1 Distribution of Device Behaviour in SIoT Networks

Device behaviour is an important factor in determining trustworthiness within the Social Internet of Things. Regular communication, successful data transmission, and consistent interaction patterns indicate reliable device behaviour, whereas suspicious communication and unauthorized activities may indicate potential security threats.

Table 1: Distribution of Device Behaviour in SIoT Networks

Device Behaviour	Frequency	Percentage
Normal communication	420	42%
Reliable interaction	250	25%
Suspicious behaviour	150	15%
Unauthorized access	100	10%
Malicious activities	80	8%
Total	1,000	100%

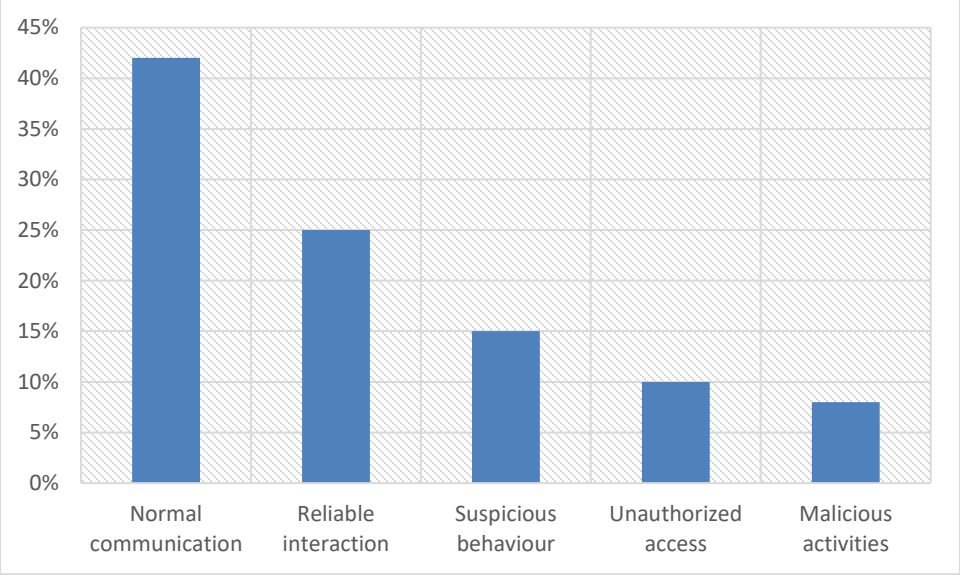


Table 1 indicates that 42% of device activities involve normal communication, while 25% represent reliable interactions. However, 15% of activities demonstrate suspicious behaviour, 10% involve unauthorized access, and 8% are associated with malicious activities. These findings highlight the importance of continuous device monitoring and intelligent trust evaluation. Machine learning techniques can help identify unusual communication patterns and distinguish legitimate devices from potentially harmful participants.

4.2 Comparative Performance of Machine Learning Algorithms

The effectiveness of machine learning algorithms is essential for developing a reliable trust management framework. Different algorithms can identify malicious device behaviour and classify network activities with varying levels of accuracy. Therefore, a comparative evaluation is important for selecting an appropriate model.

Table 2: Comparative Performance of Machine Learning Algorithms

Machine Learning Algorithm	Accuracy (%)
Decision Tree	88.5
Random Forest	94.2
Support Vector Machine	90.4
K-Nearest Neighbour	86.8
Artificial Neural Network	92.6

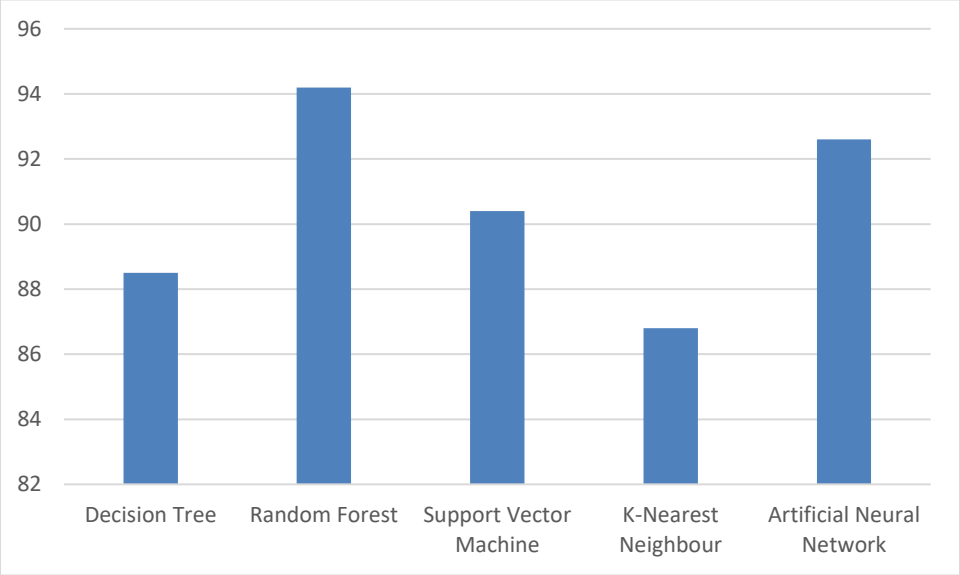


Table 2 presents the comparative classification accuracy of five machine learning algorithms. Random Forest achieves the highest accuracy of 94.2%, followed by Artificial Neural Network at 92.6% and Support Vector Machine at 90.4%. Decision Tree achieves 88.5%, whereas K-Nearest Neighbour records 86.8%. The results indicate that Random Forest provides comparatively better classification performance among the selected algorithms. Its ensemble-based learning mechanism can support the identification of complex behavioural patterns and improve the classification of trustworthy and malicious devices. However, further evaluation using precision, recall, F1-score, and false positive rate will be necessary before establishing its overall superiority.

4.3 Trust Management and Security Enhancement

Trust management plays a significant role in establishing secure communication among interconnected devices. The proposed framework evaluates device behaviour using direct trust, indirect trust, communication reliability, and reputation-based parameters. These factors help determine whether a device should be considered reliable or potentially malicious. Machine learning-based trust prediction can support dynamic trust evaluation and reduce dependence on static security mechanisms.

4.4 Detection of Malicious Activities

The identification of malicious activities is essential for protecting SIoT networks against unauthorized access, suspicious communication, and harmful interactions. Machine learning models can analyse network traffic and behavioural patterns to identify potential threats. The proposed framework will support continuous monitoring and classification of suspicious activities, allowing security mechanisms to respond more effectively to changing network conditions.

4.5 Overall Discussion

The findings presented in this study demonstrate the potential of machine learning techniques for improving trust management and security in the Social Internet of Things. The comparative results indicate that

Random Forest performs better than the other selected algorithms in terms of classification accuracy. The analysis also highlights that suspicious behaviour, unauthorized access, and malicious activities represent important security concerns in interconnected device environments. Integrating behavioural analysis, trust prediction, and malicious activity detection can strengthen the reliability of SIoT communication. Therefore, the proposed machine learning-based framework provides a useful approach for developing more secure, intelligent, and trustworthy IoT networks.

5. CONCLUSION

The present study concludes that machine learning plays a significant role in improving trust management and security enhancement in the Social Internet of Things (SIoT). The research highlights the importance of evaluating device behaviour, communication reliability, trust relationships, and malicious activities to establish secure interactions among interconnected smart devices. The comparative analysis of different machine learning algorithms indicates that Random Forest achieved the highest classification accuracy of 94.2%, followed by Artificial Neural Network at 92.6% and Support Vector Machine at 90.4%. These findings suggest that machine learning-based approaches can effectively support the identification of suspicious devices, prediction of trustworthiness, and detection of potential security threats. The proposed framework integrates direct trust, indirect trust, behavioural analysis, and reputation-based evaluation to strengthen network reliability and secure communication. Overall, the study emphasizes that integrating machine learning with dynamic trust management mechanisms can reduce security risks, improve device authentication, protect information exchange, and establish a more reliable and secure Social Internet of Things environment.

REFERENCES

1. 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.
2. Rizwanullah, M., Singh, S., Kumar, R., Alrayes, F. S., Alharbi, A., Alnfiai, M. M., ... & Agrawal, A. (2022). Development of a model for trust management in the social internet of things. *Electronics*, *12*(1), 41.
3. Kumari, S., Kumar, S. M., & KR, V. (2023). Trust management in social internet of things: challenges and future directions.
4. Alalwany, E., & Mahgoub, I. (2024). Security and trust management in the internet of vehicles (IoV): Challenges and machine learning solutions. *Sensors*, *24*(2), 368.
5. 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.
6. Moeinaddini, E., Nazemi, E., & Shahraki, A. (2025). A new approach on self-adaptive trust management for social Internet of Things. *Computer Networks*, *263*, 111187.
7. 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.
8. Roy, S. S., Sahu, B. J. R., & Dash, S. (2025). Enhanced trust management for building trustworthy social internet of things network. *IET Networks*, *14*(1), e12111.
9. Moeinaddini, E., Nazemi, E., & Shahraki, A. (2025). Enhancing security and trustworthiness in the social internet of things through incremental trust modeling. *Journal of Reliable Intelligent Environments*, *11*(4), 18.
10. 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.
11. Wei, L., Yang, Y., Wu, J., Long, C., & Li, B. (2022). Trust management for Internet of Things: A comprehensive study. *IEEE Internet of Things Journal*, *9*(10), 7664-7679.
12. Mohamed, M., & Alosman, K. (2024). A comprehensive machine learning framework for robust security management in cloud-based internet of things systems. *Jurnal Kejuruteraan*, *36*(3), 1055-1065.
13. Ghaffari, A., Jelodari, N., Pouralish, S., Derakhshanfard, N., & Arasteh, B. (2024). Securing internet of things using machine and deep learning methods: a survey. *Cluster Computing*, *27*(7), 9065-9089.
14. Liu, Y., Wang, J., Yan, Z., Wan, Z., & Jäntti, R. (2023). A survey on blockchain-based trust management for Internet of Things. *IEEE internet of Things Journal*, *10*(7), 5898-5922.
15. 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*(6), 8302-8320.