Journal of Information Systems Engineering and Management
2025, 10(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deep learning Models for Trust management in Social Internet of Things

Anciline Jenifer J[1], Piramu Preethika.S.K.[2]
[1,2] Department of Computer Science,
Vel's Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu, India

ARTICLE INFO

Received: 13 Oct 2024
Revised: 12 Dec 2024
Accepted: 23 Dec 2024

ABSTRACT

Introduction: The growing prevalence of IoT has resulted in both human-to-thing(H2T) communication and thing-to-thing(T2T) communication. In recent years, a new paradigm merging IoT with social networks has arisen, termed the Social Internet of Things (SIoT), where devices are not only intelligent but also socially conscious. Trust is an important element in SIoT and it allows reliable automatic communication between items and trust management is also an essential aspect for secure communications between IoT devices, In the dynamic SIoT environment, a traditional trust framework's static or heuristic approach is ineffective.

Objectives: To study the Deep Learning (DL) Models for trust management in SIoT and to suggest a hybrid model to predict the trustworthiness of the IoT devices in SIoT Networks.

Methods: A combined strategy is suggested in this study using Graph Neural Networks (GNN) and Recurrent Neural networks (RNN) to predict the trustworthiness of SIoT using vast high-dimensional data and detect specific trends in social communications.

Results: The finding shows that the hybrid GNN and RNN model outperforms with an accuracy of 91.8% over the standalone GNN and RNN methods.

Conclusions: The integrated model that includes both GNN and RNN techniques gives better results in terms of accuracy, precision, recall, and F1-score over the other methods assessed separately. The ability of deep learning to interpret complex multidimensional data and adapt to the highly dynamic nature of social and physical interaction is significant in maintaining trust within SIoT networks.

Keywords: Social Internet-of-Things(SIoT), Trust Management, Trustworthiness Prediction, Graph Neural Networks(GNN), Recurrent Neural Networks(RNN)

INTRODUCTION

The SIoT is a development of the IoT that blends networked smart objects with social networking characteristics. New ecosystems can be created by combining the two paradigms and enriching them. SIoT is identical to a social network of smart items. SIoT offers smart "social objects" that autonomously emulate human social behavior in everyday life. Social objects have social features that allow them to discover other items in their environment and form social interactions. It explores the SIoT in search of relevant information and services. The concept of trust and trustworthiness in social groups developed in SIoT is still quite novel and currently in a relatively early phase of exploration (Khan et al., 2021). A crucial challenge that requires careful consideration in SIoT is the establishment and long-term maintenance of trustworthy connections among various IoT components. As a result, a SIoT trust architecture must incorporate object-object interactions, social connection components, reliable suggestions, and so on(Sagar et al., 2024).

Trust management is one of the possible security strategies for boosting dependability in Internet of Vehicles (IoV) settings. There are several difficulties with protecting IoV environments from diverse threats, which motivates investigators to investigate different technologies for safety precautions and trust-based evaluation techniques.

Irrespective of these difficulties, ML has proven to be a robust solution achieving great progress in the resolution of IoV trust and security issues. According to Alalwany et al. (2024), ML has great potential as an effective approach to the security and trust issues of IoV systems.

The importance of trust in numerous disciplines and in SIoT has been explored, followed by a comprehensive examination of trust management aspects in SIoT. Furthermore, we analyze and evaluate the trust management strategies by basically dividing them into four groups based on their benefits, restrictions, trust management components and performance (Sagar et al., 2024). The DeepTrust framework, introduced by Ullah et al. in 2024, is a novel method that employs DL approaches to dynamically assess and manage reputation and trust in IoT scenarios. It demonstrates how the framework's supremacy in accurately identifying reliable and unreliable devices through extensive testing significantly improves IoT security.

Sagar et al. (2024), suggests a technique to detect complicated connections between the input and the results to predict trustable devices using artificial neural network (ANN)-based trust-SIoT architecture. Moreover, this method has been developed to acquire various essential trust metrics as input like the degree of relationship via knowledge graph embedding, flexibility of objects, trustworthy suggestions, and direct trust by combining previous and current interactions.

Xia et al. , (2019) describe an efficient method for the prediction of trustworthiness and the suggested paradigm separates trust into two distinct groups: familiarity trust and similarity trust. Familiarity trust is computed using direct trust and suggestion trust, whereas similarity trust can be evaluated using both internal and external similarity trust. Bangui et al. (2024) analyze the studies in several SIoT application domains to explore the ways of interactions with smart objects in various contexts.

Zouzou et al. (2023) extends and builds upon existing SIoT frameworks by adding a new layer consisting of trust management synthesis with contextual information, minimizing the risk of making fallacious conclusions from data that comes from IoT devices and other sources. However it is vital to note that the neighbouring devices must facilitate a secure and private ecosystem when integrated into the framework.

Roy et al. (2023) proposed an automated trust management strategy for service selection that uses trust to choose devices that are meant to communicate with other devices. The framework employs social interactions to estimate the level of trust among related devices, evaluate the overall trust of unknown devices, update observed trust levels on a regular basis, and eliminate malicious nodes from the network. The proposed method uses the SIoT to manage trust. The majority of research focuses on either physical traits or social connections, but infrequently on both. To improve the accuracy of trust prediction, a hybrid model that combines social and physical factors is proposed.

OBJECTIVES

The major aspect of the study is to explore and improve techniques for assessing the trustworthiness of IoT devices in SIoT networks. SIoT is a concept, in which IoT devices communicate with one another and establish social relationships based on mutual ownership, use, or functionality. The major objectives of the study is to

- Explore the various methods to predict the trustworthiness of the IoT devices in SIoT.
- Suggest a hybrid model using GNN and RNN to predict the trustworthiness of the IoT devices in SIoT networks.

The GNN and RNN has been employed for the following two reasons

- GNN is used for obtain the complex relationships and associations between IoT devices in a SIoT setting and it has the ability to effectively handle graph-based data that depicts the structure of the network.
- RNNs' is used to manage temporal data and it makes them appropriate for acquiring the dynamic characteristics of trustworthiness in IoT communications.

METHODS

This section provides the hybrid GNN and RNN for trustworthiness prediction of IoT devices in the SIoT environment. The efficiency of the hybrid model is compared with GNN and RNN separately.

Data Collection

The data collected from the SIoT networks includes behavioral logs , network structure , external factors and historical trust scores. An example sequence input data is shown in Table 1

Table 1: Sequence Data

Time step	Interaction success	Response time	Error rate	Device Status
1	1	49 ms	0.1	Active
2	0	210ms	0.5	Active
3	1	45 ms	0.2	Active

Graph Neural Networks (GNN)

GNN, an innovative and rapidly expanding family of neural network models, are capable of recording intricate relationships within sensor architecture and have been proved to reach state of-the-art outcomes in several IoT learning tasks(Zhong et al.,2023) This technique uses both a graph's edge properties and topological data for network detection of breaches in IoT networks(Wang et al., 2022). GNNs are ideal to forecast the reliability of devices in SIoT networks given that they employ graph topologies to simulate node connections and interactions.

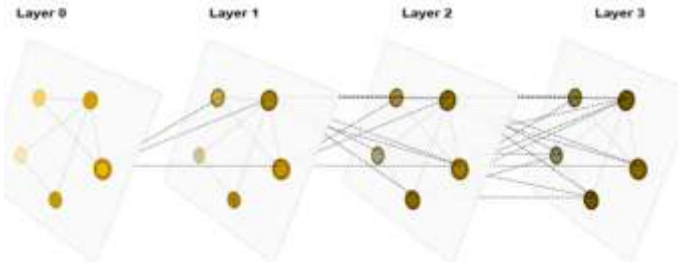

Figure 1 GNN

The SIoT networking is depicted by the graph G=(V,E), where V represents the collection of nodes indicating IoT devices and E is the set of edges that describe relationships. Each device (node) has characteristics such as activity records, interaction patterns, and security measures. Edge Specifications are optional that may signify the strength of relationships or trust background. The aim is to estimate a trustworthiness score (Tv) for every node (v) or a paired credibility value for edges (e). In the figure 1 , nodes are the IoT devices, and edges represents the relationships and device metrics like latency, response time, failure are the node features and relationship metrics like communication frequency indicate the edge features(Li et al., 2023).

Recurrent Neural Networks (RNN)

RNNs are particularly suitable for threat detection in the IoT, as they can evaluate sequential data, which is frequent in IoT traffic over networks(Thakur et al., 2023). The overall steps for RNN are as follows

- Select the input data which includes interaction history of the IoT devices like success or failure indications and behavior of devices like anomalies and response times.
- Extract the meaning features form raw data like success rate, ratings, and time intervals between interactions
- Split the data into sequences of equal length T and output the trust score at time T
- Then normalize to scale the features to a standard range for consistent model training
- Define the network structure as depicted in figure 2

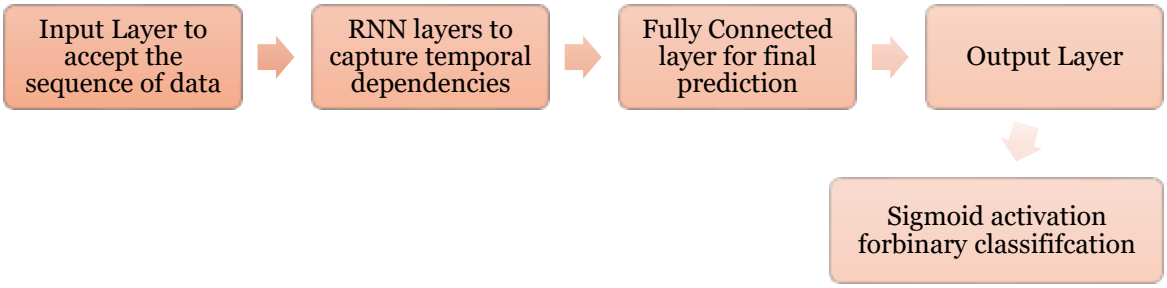

Figure 2. RNN for trust prediction

- Initialize the model by defining the input dimensions and RNN
- Train the model using the Adam optimizer
- Assess the model using performance indicators like accuracy, precision, recall and f1-score
- Further hyperparameter tuning can be done by modifying the number of hidden layer and units, sequence length, learning rate and batch size.
- Deploy the model

Hybrid Model (GNN and RNN)

Integrating GNN and RNN for predicting trustworthiness in IoT devices takes advantage of the features of both models. GNNs represent the relational and geometrical structure of IoT networks, whereas RNNs depict the sequential behavior of devices across time. This hybrid method is particularly successful in the SIoT, where trust relies not just on device behavior but also on network relationships and interactions. The workflow of the hybrid model is shown in figure 3.

Figure 3. Workflow of hybrid model to predict trustworthiness

- GNN defines the IoT network as a network of lines, with nodes representing devices and edges representing connections (such as interactions, closeness, and trustworthiness ties).
- It retrieves structural and historical context from surrounding nodes/devices.
- RNN processes the chronological order of device events or activities and tracks temporal trends regarding particular device efficiency over time.
- In Fusion Layers, GNN and RNN results are combined to make a final trustworthiness prediction.

RESULTS

The assessment of GNN, RNN, and a hybrid GNN-RNN model for predicting trustworthiness in IoT devices is shown in table 2. The measures examined include accuracy, precision, recall, and the F1-score(Kosta et al., 2023). The experiments were carried out in a colab environment using python.

Dataset Description:

IoT-23 Dataset is used for the trustworthiness prediction in SIoT. IoT-23 is a data collection including network activity from IoT devices. It has 20 malware catches in IoT devices and 3 grabs of benign IoT device traffic. Its rationale is to offer academics with a big dataset of valid and tagged IoT infections with malware and benign traffic to help them develop ML techniques. Avast Software financed this dataset and the research. The virus was allowed to get connected to the internet. This dataset is useful for distinguishing between trustworthy and untrustworthy devices by analyzing their network activity.

Performance Metrics

Accuracy is a performance indicator used to assess the efficacy of a ML model in classification tasks. It calculates the percentage of true predictions generated by the model out of all forecasts. Accuracy is often used, however it

may not always be the optimal statistic, particularly in unbalanced data sets. The accuracy computation is given by the equation (1).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

If the model shows high accuracy with the set data, it implies that the model is functioning well, whereas lower levels show inefficiency in its predictions. However, this could be erroneous if the data being collected is biased.

Precision is a metric that quantifies the strength of any classification model. It is calculated using the following formula: precision is given in equation (2).

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

Recall measures the ability of the model to locate each relevant instance in that dataset. It is crucial, for instance, in situations where ignoring positive instances (false negatives) is costly. The formula for calculating Recall is given in equation (3)

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

The F1 Score is an indicator of performance that utilizes Precision and Recall to assess a classification algorithm. It is especially beneficial when the dataset is skewed and you need a statistic that takes into account both false positives and false negatives

$$F1 - Score = 2 * \frac{precision*recall}{precision+recall} \quad (4)$$

In order to estimate the trustworthiness of IoT devices in SIoT networks, the table 1 contrasts the performance of three algorithms: GNN, RNN, and a Hybrid GNN-RNN.

Table 2 Performance Analysis

Prediction Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score(%)
GNN	86.6	84.6	77.3	79.1
RNN	83.3	80.5	76.7	78.2
Hybrid GNN-RNN	91.8	89.1	87.4	89.2

From table 2, it is clear that the hybrid GNN-RNN performs better in predicting the trustworthiness of IoT devices. The hybrid model improves accuracy by using GNNs to prevent misclassifications caused by outlier associations in the graph. The most effective outcome is shown by the Hybrid GNN-RNN model, which combines the advantages of both GNN (capturing intricate relationships) and RNN (managing temporal patterns). Although GNN and RNN work well separately, the hybrid technique performs more effectively, especially in accuracy (+5.2% over GNN, +8.5% over RNN) and recall (+10.1% compared to GNN, +10.7% compared to RNN). This demonstrates the benefit of integrating models to handle the complex elements of predicting trustworthiness in SIoT networks.

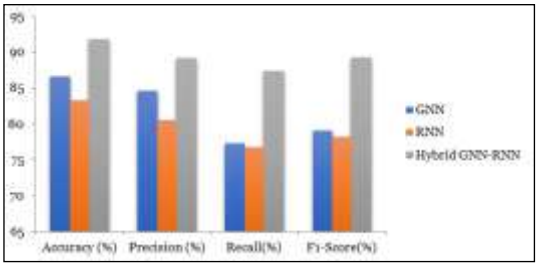

Figure 4 Methods vs Measures

Figure 4 presents the performance chart for GNN, RNN, and the proposed hybrid GNN techniques. It is found that the hybrid GNN-RNN outperforms the other two methods. GNN effectively captures connections and structural interconnections in IoT networks. It moderates recall due to its weak capacity to accurately predict temporal

activity. It works well in environments where data with relationships (e.g., topology and links) is prevalent. RNN excels at detecting sequential relationships in device activity across time. It performs poorly on measures that rely on relational context, such as accuracy, since it does not naturally describe network structure. It is suitable for cases with a high volume of time-series data data and a little attention to network interactions. The hybrid GNN-RNN provides optimal performance by integrating relational and temporal modelling characteristics. Increased accuracy and recall suggest a more consistent ability for accurately identifying trustworthy and untrustworthy devices. It is ideal for IoT applications where network interactions and temporal device activity are important. Employ oversampling or weighted loss to address skew in trust ratings for data imbalance. Regular updates to the model are necessary to account for evolving device behavior. and the model justification for choices made to increase user confidence.

CONCLUSION

The study suggests a hybrid DL framework based on GNN and RNN for trustworthiness prediction of IoT devices in SIoT. In terms of the performance metrics, the results show that the proposed hybrid model outperforms the GNN and RNN approaches independently. DL models have considerable potential for managing trust in SIoT networks because of their capacity to assess complicated multidimensional data and adjust to the changing nature of social as well as physical interactions. However, applying them effectively necessitates overcoming problems such as quality of data, interpretability, and utilization of resources. Future studies ought to focus on improving model explainability, constructing compact and secure architectures, and collecting vast, varied datasets for training more robust models. Addressing these difficulties will allow the efficient deployment of deep learning to develop safe, reliable, and scalable SIoT ecosystems. The future work includes Improving the interpretability of DL models in order to increase user trust and discover the fundamental causes of risks and also to combine DL and block chain to provide safe, identifiable device interactions.

REFERENCES

[1] Alalwany, E., & Mahgoub, I. (2024). Security and Trust Management in the Internet of Vehicles (IoV): Challenges and Machine Learning Solutions. *Sensors*, *24*(2), 368. https://doi.org/10.3390/s24020368

[2] Bangui, H., Buhnova, B., Kusnirakova, D., & Halasz, D. (2023). Trust management in social Internet of Things across domains. Internet of Things, 23, 100833.

[3] H. Xia, F. Xiao, S. -s. Zhang, C. -q. Hu and X. -z. Cheng, "Trustworthiness Inference Framework in the Social Internet of Things: A Context-Aware Approach," *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, Paris, France, 2019, pp. 838-846, doi: 10.1109/INFOCOM.2019.8737491.

[4] Konsta AM, Lafuente AL, Dragoni N. A survey of trust management for Internet of Things. IEEE Access. 2023 Oct 25.

[5] Li, B., Lin, Y., & Khan, I. A. (2023). Self-supervised learning IoT device features with graph contrastive neural network for device classification in social internet of things. IEEE Transactions on Network and Service Management, 20(4), 4255-4267.

[6] M. C. Zouzou, E. Benkhelifa, H. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," *2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS)*, Valencia, Spain, 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510

[7] Roy, S. S., Sahu, B. J. R., & Dash, S. (2023). Enhanced trust management for building trustworthy social internet of things network. IET Networks.

[8] Sagar, S., Mahmood, A., Sheng, Q. Z., Zhang, W. E., Zhang, Y., & Pabani, J. K. (2024). Understanding the trustworthiness management in the social internet of things: A survey. Computer Networks, 251, 110611

[9] Sagar, S., Mahmood, A., Sheng, Q.Z. (2024). Towards Trustworthy Object Classification in the SIoT Network. In: Towards Resilient Social IoT Sensors and Networks. Smart Sensors, Measurement and Instrumentation, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-031-60701-1_5

[10]Thakur, D., Saini, J. K., & Srinivasan, S. (2023). DeepThink IoT: the strength of deep learning in internet of things. Artificial Intelligence Review, 56(12), 14663-14730T.

[11] 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] W. Z. Khan, Q. -u. -A. Arshad, S. Hakak, M. K. Khan and Saeed-Ur-Rehman, "Trust Management in Social Internet of Things: Architectures, Recent Advancements, and Future Challenges," in *IEEE Internet of Things Journal*, vol. 8, no. 10, pp. 7768-7788, 15 May15, 2021, doi: 10.1109/JIOT.2020.3039296

[13] Wang, G., Wang, H., Gong, J., & Ma, J. (2024). Joint item recommendation and trust prediction with graph neural networks. Knowledge-Based Systems, 285, 111340.

[14] Zhong, M., Lin, M., Zhang, C., & Xu, Z. (2024). A Survey on Graph Neural Networks for Intrusion Detection Systems: Methods, Trends and Challenges. Computers & Security, 103821.