ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 1, 2024

TRUST–SIOT: TOWARDS TRUSTWORTHY OBJECT CLASSIFICATION IN THE SOCIAL INTERNET OF THINGS

B.Sandhya, Professor, Department Of CS SICET, Hyderabad
A.Navya, Boddu Chandra Shekar, Chintala Bharath Reddy, Gundlapally Sujith Kumar
UG Student, Department Of CS, SICET, Hyderabads

Abstract —

The recent emergence of the promising Social Internet of Things (SIoT) paradigm is the result of intelligently merging social network concepts with Internet of Things (IoT) objects (also referred to as “things”) to attempt to unravel the challenges of network discovery, navigation, and service composition. This is achieved by facilitating socialization of IoT objects with each other, i.e. similar to social interaction between human beings. A fundamental issue that requires careful attention is to create and over time maintain trusting relationships between these IoT objects. Therefore, the trust framework for SIoT must include object-object interactions, aspects of social relationships, credible recommendations, etc., but existing literature has only focused on some aspects of trust by primarily relying on conventional approaches that govern linear relationships. between input and output. In this paper, a trust framework based on the Trust–SIoT artificial neural network was proposed to identify complex nonlinear input-output relationships in an effort to classify trusted objects. In addition, Trust–SIoT was designed to capture a number of key trust indicators as input, i.e., direct trust by integrating current and past interactions, object reliability and benevolence, trusted recommendations, and degree of relationship using a knowledge graph. inserting. Finally, we conducted extensive experiments to evaluate the performance of Trust–SIoT vis-a-vis state-of-the-art heuristics on two real datasets. The results show that Trust–SIoT achieves higher F1 and lower MAE and MSE scores.

Index Terms – Trust Management, Social Internet of Things,Knowledge Graph Embedding, Social Relations, Reliability,
Leniency.

I. INTRODUCTION

RECENT advances in computing technology have seen a huge number of smart objects (e.g., smart meters, smart watches, and smart refrigerators) connected to the Internet to form the Internet of Things (IoT) [1]–[3]. In addition, these smart objects are equipped with sensing, processing and communication capabilities, enabling them to provide various applications and services that are expanding in various fields, including personal, industrial and commercial [4] [5] . With the proliferation of IoT applications from smart homes to smart factories. smart cities. to e-Health, the number of IoT objects (i.e. devices) is rapidly increasing, which limits network discovery and navigation

Mapping the social structure of humans and physical (i.e., IoT) devices (see Figure 1) has led to the emerging paradigm of the Social Internet of Things (SIoT) and paved the way for the next generation of the Internet of Things [8]. In addition, the mapping includes three distinct relationships (ie, user-object relationships, object-object relationships, and user-user relationships). In SIoT, objects have the potential to socialize by establishing social relationships with each other autonomously based on rules defined by their individual owners [9]. The evolution of SIoT can be envisioned as trillions of objects acting as autonomous agents (i.e. requesting and providing services) with a number of benefits including, but not limited to, ensuring efficient discovery of objects and information in a trust-oriented manner, network scalability similar to human beings, building trust by incorporating interactive behavior among friends (or objects) and the use and extension of existing social network models for SIoT networks.By leveraging social relationships with IoT objects, SIoT has paved the way for the next generation of the Internet of Things.

However, maintaining trusted relationships, as well as concerns related to security, privacy and trust, may limit the importance of the SIoT paradigm. For example, in a SIoT scenario, a service requester (or trusted entity) has the responsibility to monitor the trustworthiness of service providers (or administrators) that provide the requested service; however, the possibility that a misbehaving object provides false services or false recommendations about a manager to gain an advantage for a set of services can disrupt the availability and integrity of SIoT services. Although some researches have presented cryptographic and non-cryptographic solutions to solve these problems [10] [11], security issues such as trust and reputation are difficult to handle with such solutions. As a result, an effective SIoT trust management system is required to deal with misbehaving SIoT objects by restricting their services and selecting only trusted and trusted objects before relying on their services.The motive for introducing trust management for SIoT is clear from the observations made. Several studies have been proposed to address the issues associated with trust management. However, most of these studies do not consider a thorough study of SIoT fundamentals, such as 1) selecting reliable SIoT-based metrics, 2) only considering the static characteristics of SIoT relationships (e.g., ownership, location), and 3) using a traditional approach (i.e., linear relationship) to map inputs and outputs for trust management.In this paper, we proposed a trusted object classification framework, known as Trust–SIoT, which uses the concept of social trust theory to address the above weaknesses. The main contributions of the proposed article are as followsThe Trust - SIoT (Trust - SIoT) classification framework is designed to exploit the social characteristicsobjects in terms of direct metrics of trust, reliability and benevolence, trusted recommendations and degree of relationships.

We are building SIoT

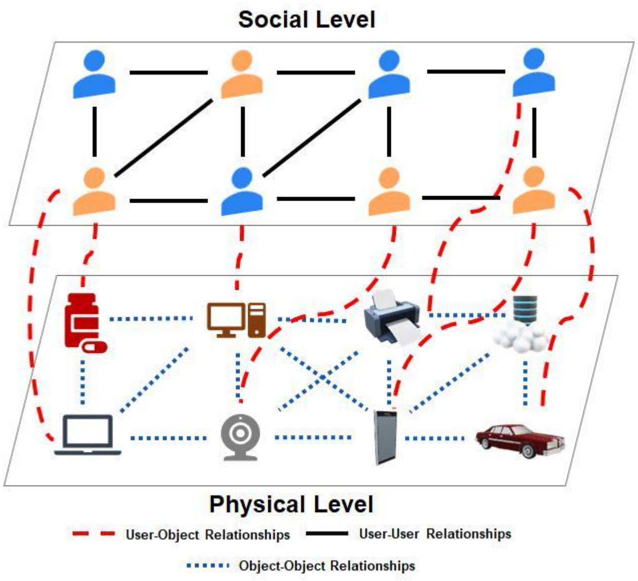


Fig. 1: Depicting the SIoT relationships

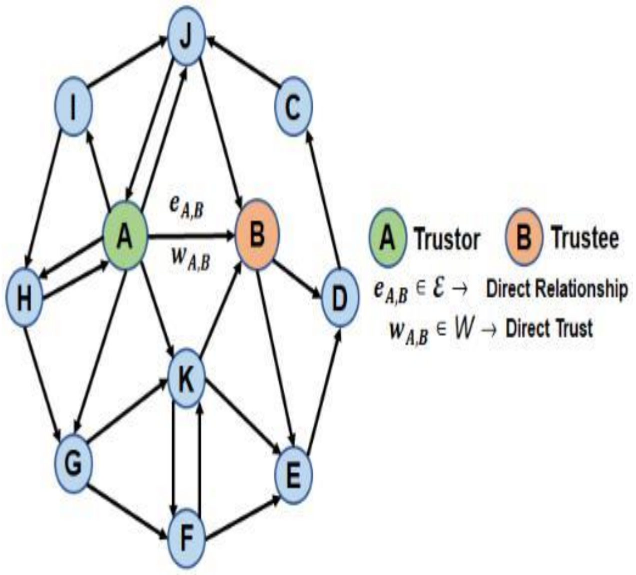

J
I
C
A
B
H
D
K
G
E
F
$e_{A,B}$
$w_{A,B}$
A Trustor
B Trustee
$e_{A,B} \in \mathcal{E} \rightarrow$ Direct Relationship
$w_{A,B} \in W \rightarrow$ Direct Trust

Fig. 2: SIoT network as a directed graph G = (V; E; W)

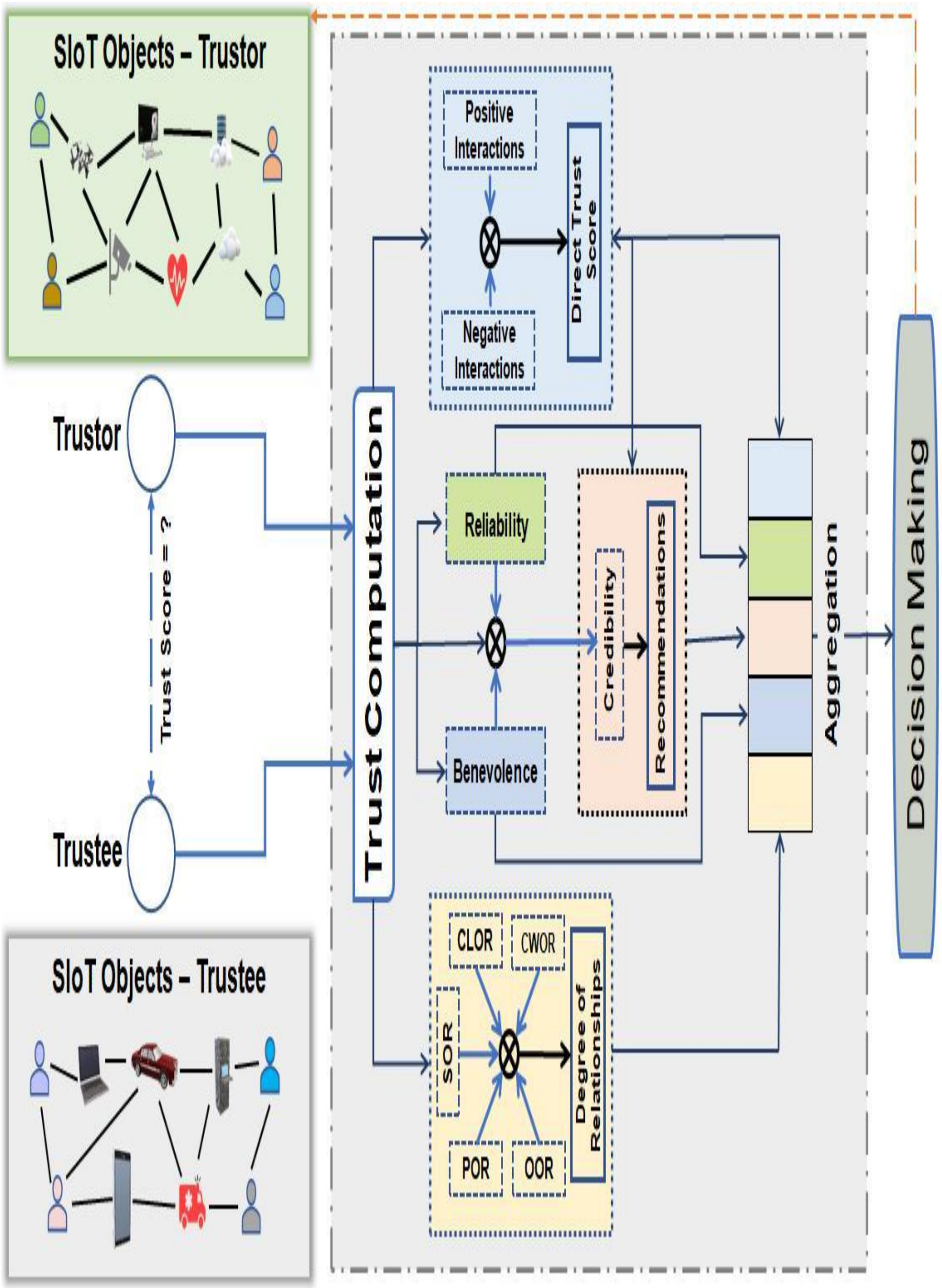
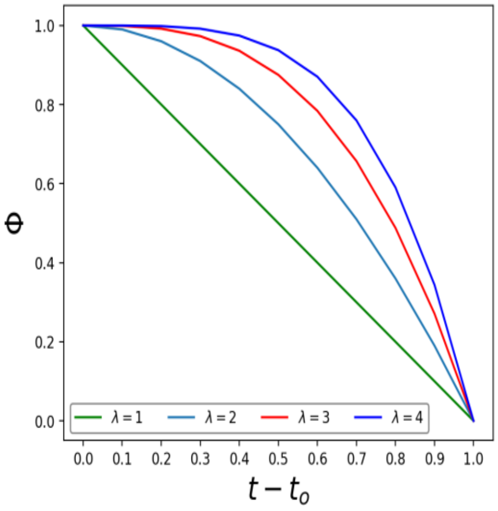


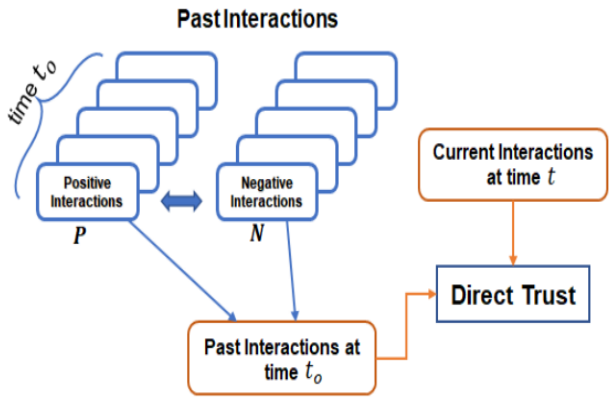
Fig. 3: Illustration of Trust–SIoT framework (represents concatenation)

TABLE I: Summary of notations

Notatio n	Description
P	Positive (Successful) Interactions
N	Negative (Unsuccessful) Interactions
B	Benevolence
R	Reliability
CR	Credibility
K	Number of credible objects
	Trust Factor
	Rate of Trust Factor
f	KGE scoring function
L	Cross Entropy Loss
C D oR	Context-aware Degree of Relationships
DT M	Direct trust of trustor-trustee pair
RT M	Recommendations for trustee
T	Final Trust Score

IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. , NO. , APRIL 2022 5





Data preparation and conclusion:

Since the selected datasets do not contain information about SIoT relationships between objects, which is a core component for any SIoT network, we extracted information about SIoT relationships from the Social Dataset3. The social dataset contains information about real IoT objects deployed in the city of Santander, Spain, and there are 16 of them in total; 216 IoT objects. In addition, this dataset contains five different types of SIoT relationships (i.e., CLOR, POR, OOR, SOR, and SOR2) between IoT objects that connect them into a SIoT network and the service information requested by these objects. We extracted the subnet relationship information of this dataset to integrate it with Advogato and BTC-Alpha by selecting objects to increase the probability of objects interacting with each other. The merging takes place in three steps: 1) converting the SIoT dataset to the SIoT graph, 2) selecting the data subnet to match the number of nodes for each Advogato and BTC-Alpha dataset, and 3) merging the data subnet. SIoT data network with both Advogato and BTC-Alpha dataset. Finally, we mapped the labels of the merged datasets into three fT rustworthy classes; N neutral;

CONCLUSION

This study examines various machine learning approaches employed in the field of cybersecurity for the purpose of anomaly detection. This study investigates the utilization of diverse machine learning techniques, encompassing supervised learning, unsupervised learning, deep learning, and rule-based methods. This study examines the practical applications of cybersecurity in several domains. Furthermore, this underscores the significance of feature selection, engineering, and assessment metrics in the development of resilient anomaly detection models. In conclusion, a comprehensive evaluation of the strengths and limits of different methodologies is essential in order to facilitate the selection of relevant approaches by both present and future researchers.

REFERENCES

[1]. "Machine Learning Techniques in Cybersecurity." Encyclopedia. Retrieved from https://encyclopedia.pub/entry/25675.

[2]. Abdullah, A. H., Ahmed, M. H., & Wahab, M. H. A. (2021). A Comparative Study of Network Intrusion Detection Techniques Using NSL-KDD Dataset. IEEE Access, 9, 91924-91942.

[3]. Akhtar, S., Faisal, M., Ahmad, S., & Rho, S. (2020). Machine learning-based ransomware detection: State-of-the-art and future research directions. Journal of Network and Computer Applications, 153, 102539.

[4]. Akinyele, J. R., Gao, K., & Zhu, S. (2015). Insider threat detection using log analysis and machine learning. International Journal of Information Security, 14(5), 403-415.

[5]. Alawami, A. K., Khan, M. K., & Kiong, T. E. (2020). Insider threat detection: A review and research directions. Journal of Network and Computer Applications, 153, 102531.

[6]. Alazab, M., Hobbs, M., & Abawajy, J. (2018). A survey of botnet detection techniques. Journal of Network and Computer Applications, 110, 60-71.

[7]. Alzahrani, B., Zulkernine, M., & Alazab, M. (2020). Machine learning-based intrusion detection techniques for securing industrial control systems: A review. Computers & Security, 88, 101628.

[8]. Bhattacharya, S., Gupta, P., & Chatterjee, J. (2021). A comparative study of machine learning algorithms for malware detection. Multimedia Tools and Applications, 80(10), 14935-14957.

[9]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 15.

[10]. Chiong, R., Lee, V. C., & Zhou, L. (2017). Anomaly detection in cyber security: A machine learning approach. In Machine learning paradigms: Advances in data analytics (pp. 81-112). Springer, Cham.

[11]. Demertzis, K., & Karampelas, P. (2020). A review of anomaly detection techniques in financial markets: An application to emerging markets. Expert Systems with Applications, 146, 113172.

[12]. Dhamecha, T. I., & Thakkar, P. (2020). A Comprehensive Review on Anomaly Detection Techniques using Machine Learning. International Journal of Advanced Research in Computer Science, 11(4), 44-51.

[13]. Fawaz, H. I., Forestier, G., Weber, J., Idoumghar, L., & Muller, P. A. (2018). Data augmentation using synthetic data for time series classification with deep residual networks. arXiv preprint arXiv:1808.08467.