1Chethan Raj C

2Dr Hanumanthappa J

Implementation of Trust Model for Social Internet of Things Using Centrality Feed Forward Networks

Abstract: - Recent advances of Internet of Things (IoT) lead to the most promising paradigm called Social Internet of Things (SIoT). These techniques are considered the strong amalgamation of the social networking features with the IoT objects. These networks are characterized by facilitating the IoT objects to establish the social networking between each other. In SIoT, an interconnection of networks formed by considering the important features such a object-object interactions, social relationship, reliable recommendations and mandates the careful attention towards the strong trustworthy connections. Hence Intelligent Trust Model Identification Model System (ITMIS) is required for the SIoT networks to identify the misbehaving objects by selecting only the reliable, credible and trustworthy objects before relying on the services provided by them. However, existing frameworks truly relay on the conventional approaches that is based on linear relationship between the inputs and outputs. These methods may lead to the high misclassification ratio of selecting the untrusted devices that even may cause untrust process in an application. To overcome this problem, in the proposed research work the novel ITMIS which ensembles the non-linear centralities relationships with the architecture Extreme Feed Forward Neural Networks (EFFNN) with the combination of hybrid algorithm of Long Short Term Memory (LSTM) and Gated Recuurent Unit (GRU) for the better accuracy compare with the existing model. The proposed model captures the number of key trust metrics based on centralities measurements and envisages the EFNN to classify the trusty and non-trust objects. The extensive experimentations are conducted using the real world datasets and various trust metrics were evaluated and compared with the other state-of-the-art trust learning models. The results demonstrate that the proposed model has outperformed with the other existing models by maintaining the accuracy of 95% to 94% with the decreasing untrusted rates and It illustrates conclusively that the LSTM's use of enhancing ensemble characteristics has shown to be more advantageous. While other models, like E-LSTM (90%) to 80%, Stacked LSTM (85% to 80%), SVM (85% to 79%), KNN (75% to 68%), and RF (65% to 58%), exhibit decreasing efficiency, the proposed approach illustrates that it is more productive as well as efficient for building an intelligent trust classification system that is appropriate for establishing trusted SIoT network communication.

Keywords: Social Internet of things, Trust and untrust nodes, Extreme Feed Forward Neural Networks, Long Short Term Memory, and Gated Recuurent Unit

I. Introduction

The emerging paradigm represents a burgeoning trend in technology, functioning as a network that interconnects numerous devices to the internet. SIoT is intricately linked with sensors and actuators designed to monitor various human aspects, thereby supporting a multitude of applications aimed at fulfilling diverse services tailored to specific requirements. A prime utility of IoT lies in establishing networks of resources with a social dimension, facilitating the identification of social relationships to address tasks efficiently. The integration of IoT with social networks fosters extensive interactions among a vast array of objects within a network. In SIoT, objects exhibit diverse forms of relationships with other objects prior to establishing actual communication, encompassing direct relationships as well as indirect ones, often referred to as direct trust and indirect trust, respectively. The mutual interaction among heterogeneous objects presents numerous challenges, including issues related to trust, security, and other processes. These challenges necessitate the establishment of trusted communication mechanisms before actual message transmission within the SIoT network.

Trust serves as the cornerstone for interactions among nodes or objects interconnected via the SIoT network. Objects rely on trust to delegate tasks to other objects within a specified timeframe, with trust scores, whether direct or indirect, amalgamating to form the final evaluation. Despite numerous proposed trust evaluation models, many have faltered in adapting to the dynamic environment of SIoT. The RB-SIoT model, however,

[1]Research Scholar, Department of Studies in Computer Science, UoM, & HoD, VTU, Karnataka, India

[1]chethanraj016@gmail.com

[2] Professor, Department of Studies in Computer Science, ManasaGangothri, UoM, Mysore. Karnataka, India

[2]hanumsbeprof@gmail.com

represents a notable advancement in constructing a trust model for SIoT networks, particularly in autonomous interactions between nodes. By using a machine learning technique to use characteristics including cooperativeness, resilience, and information gain, the RB-SIoT model shows major advantages. The identification of influential nodes using the suggested algorithm will be covered in detail in portions that follow.

As preparation datasets, the recommended approach can employing modified centrality behaviours when combined with distrustful or malicious information. This work uses improved centrality measures to determine the level of trust, which results in the introduction of additional feature vectors to each node.. Subsequently, utilizing EFNN learning models with LSTM and GRU based on the training datasets, the paper endeavors to discern classification/prediction rules and categorize the significance of trusted objects interconnected in an IoT networks. The ensuing discussions elucidate the significance of cooperation among nodes through proper ties, defining the efficacy of the proposed system. The featuring diverse sets of attributes among cooperative nodes, undergoes evaluation to assess trust using the proposed model, ensuring proper utilization of trustworthiness. Furthermore, the proposed model elucidates methods for discerning the intrinsic value of objects.

This research continues by outlining the community-based Network of Devices strategy using robustness approaches. The review of similar work that describes methodology and data object analysis to differentiate between competitive and ineffective entities occurs shortly. The paper then proceeds further insight on the architecture and technique, explaining how to integrate IoT with a feature subset of data that has been modified to fit a mathematical model in order to facilitate implementation. In addition, a comparative analysis of several characteristics, including cooperativeness, cluster coefficient, centrality, information gain, and closeness, is carried out to provide assessment metrics that support the improvement of trust assessment and the extraction of insights from the data.

II. RELATED WORKS

Subhash Sagar et al.[1] Focuses on trust frameworks for SIoT, emphasizing non-linear interactions and introduces Trust-SIoT framework for collecting trust metrics. Magdich et al. [2] Addresses evolving SIoT node contexts with the CTM-SIoT model. Uses machine learning for identifying malicious nodes, enhancing trust mechanisms. Latif et al.[3] Introduces ConTrust model for context-dependent trust management in SIoT. Emphasizes distinguishing between malicious and trustworthy objects. Athira et al.[4] Studies dynamic network architectures in SIoT, focusing on trust. Employs machine learning techniques for trust value classification. Goswami et al.[5] Explores trust in SIoT communities, using machine learning for aggregate trust scoring. Sagar et al.[6] Proposes a trust computational model for SIoT, employing machine learning for trust score aggregation. Kazia et al.[7] Classifies false news detection methods and their applications in SIoT. Shaji et al.[8] Integrates SIoT and big data, utilizing machine learning for classification. Ali-Eldin et al.[9] Utilizes hybrid approach for trust computation in social IoT scenarios. Magdich et al.[10] Proposes a Trust Management model for SIoT, emphasizing defense against trust-related attacks. Ortiz et al.[11] Discusses trust models in IoT for network navigability and scalability. Highlights the importance of trust in SIoT for various domains.

Trust management in SIoT is crucial but faces challenges regarding trust metric definition, trust model effectiveness, and social object relationships. Social interactions significantly affect trust values alongside service-based interactions. Existing studies have not comprehensively addressed trust issues in SIoT networks, especially considering all network information and diverse relationships. Establishing trustworthy relationships is vital for successful cooperation among objects, necessitating efficient trustworthiness computation processes. Overall, the literature underscores the importance of robust trust management mechanisms in SIoT networks, considering the dynamic nature of interactions and the impact of social relationships on trust values.

III. ARCHITECTURE OF TRUST MONITORING FOR SIoT

A. ARCHITECTURE AND SYSTEM DESIGN

The design of highly efficient feature information systems that can distinguish between regular and critical nodes is the key objective of the present study. Various prominence metric uncovering approaches are made to use in writings to show the relevance of the nodes. The proposal for research offered instances of ways to apply the boost in the number of precedence metrics in identifying nodes with impact as precisely as feasible.

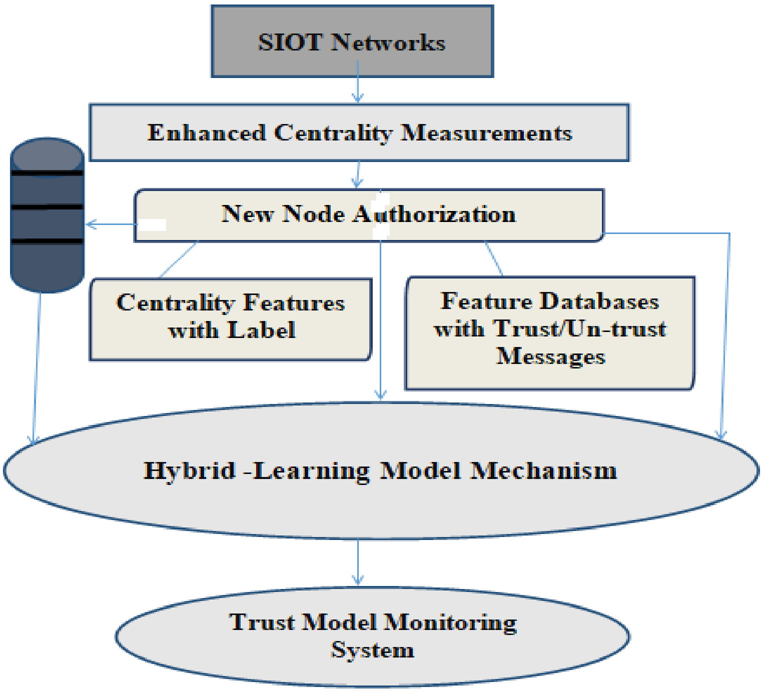
SIOT Networks
Enhanced Centrality Measurements
New Node Authorization
Centrality Features with Label
Feature Databases with Trust/Un-trust Messages
Hybrid -Learning Model Mechanism
Trust Model Monitoring System

Figure 1: Proposed Architecture Trust Model

The trust model's architecture is shown further in Figure 1, which knowledge originates from an assortment of smart gadgets, such computers, apparatus, sensors, controls, and connected devices, or SIoT networks. Instead of choosing the complete set of data from the real-time dataset, different relevance reviews take into consideration the authorization credentials of the latest node as well as the data provided by the devices. In the present instance, the feature selection model aids in extracting the necessary feature data from the provided dataset. After these data are gathered and evaluated using the characteristics of the proposed model, a feature data set is formed using the results. A interpersonal network's reputation is able to be assessed based on a variety of criteria, including knowledge gain, collaboration, endurance, intimacy, prominence, or solidity.

These factors have a big impact on system confidence. By gathering the information, the acquired knowledge minimizes the traits in a data set with refinement. In terms of features, an individual is able to examine at how a node communicates with other nodes in the network or with other nodes itself. By separating the appropriate components by considering the relationships between objects, events, and individuals, the complexity of the data set for each object in the context is minimized. Through this social network, entities with well-connected ties can maintain interactions to promote productive interaction between individuals, enabling things to cater as well as recoup from major problems on any variety. Another feature that is useful for collecting or forming a chain of events with greater intimacy involving the ways that things react to it, relate, and perceive each other is their proximity.

An object's interactions with other objects primarily negate the appropriate connection in a system of objects. Following the acquisition and usage of remaining data as resources, traits are determined in order to alter the data, which is then needed by specific methodologies. This method contributes to a reduction in the total number of attributes by offering new features derived from the available data. Once the best predictors have been chosen, the data is applied to those for the purpose to split information out. Hazards are computed by fitting a hierarchy to the data; if this is not the case, the step is repeated until the point of no development arrives. Input scuffing is done in order to make input acceptable; adhering to vicinity forecast, if its outcomes suit standards, proceed on to the subsequent phase before the specified amount of trials has been accomplished. There is a link between an estimate technique, data collection, and choices for features.

A system interactivity plane is in responsible for maintaining network assessment for different data varieties using dissimilar methods and training for create to various data while each method generates data in a unique way. Data objects have been trained provided to gauge trust using widely used models, such as the significance factors and coefficients of every data point as an interaction. The content format layer acts as that is the last section, is able to handle three various types of data: informal, unorganized and regular. Once the appropriate trust value was established, the data may be received through an application. Some large-scale data are utilized for figuring out the valid and important information for an assessment of confidence among entities. As an outcome, the complex structure of the belief system is depicted above, exhibiting how preliminary information is derived and extracted from various sources in order to manipulate and analyze an appropriate number of knowledge elements to detect trends in data that are then turned into trained in and knowledge provided can understand the functioning of devices and form choices. Through this community of people, one could enhance interaction with others and sustain interactions between events through establishing accessible connections allowing a few react as well as emerge from widespread problems as every sort.

The below diagram highlights how one node in a group of devices acts as a parent, child, or sibling based on its behaviors and configuration.

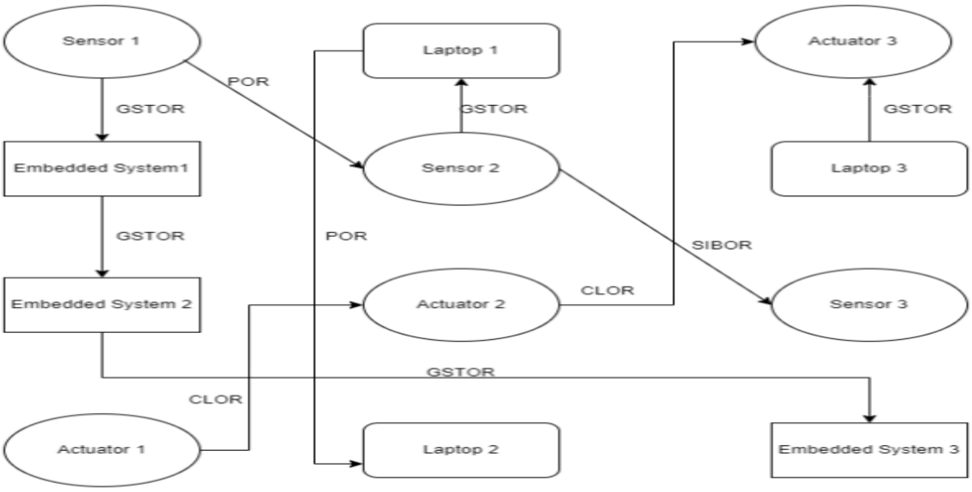

Figure 2: Object Relationship Type Model

Computers, electronic gadgets, and sensors are illustrations of systems embedded into objects. These gadgets are taken for consideration while gathering information for communicating via nodes. Various actuators and sensors utilized that are linked to the component's correlation system perform the process of obtaining data. An object such as an a device is an electronic device that employs an embedded system to operate an application and handle its output. It acquires data from sensor that is being tested and activator devices.

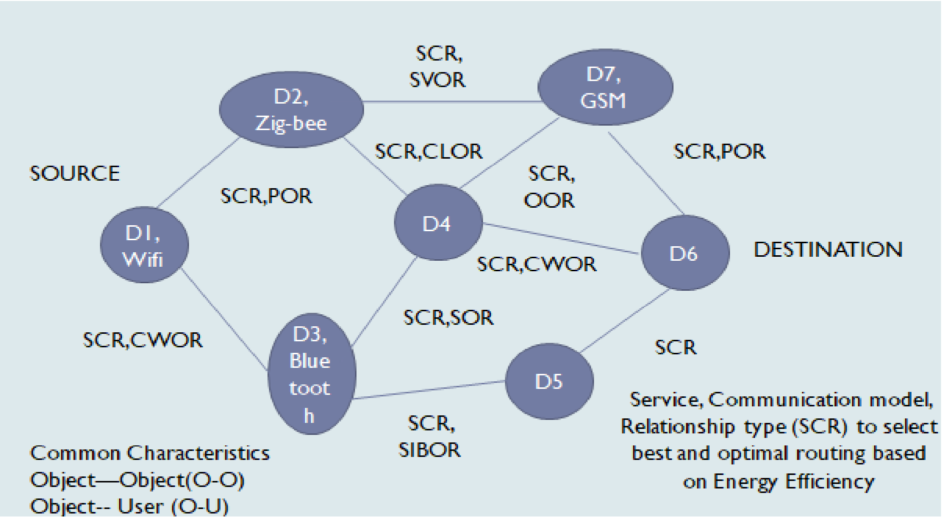

Figure 3: Process Diagram of Trust Model

The fig 3 describes the SIoT process trust model diagram, where the data is collected from the different devices and each device establishes the relationship between other devices before the start of the communication with reference to the service requested and composed followed by the trusted value is measured using machine learning approach that evaluates that device is trusted or not.

B. PROPOSED ALGORITHM

The model and algorithm is implemented for SIoT dataset of ADVOGATO Network Data Statistics

Algorithm: Hybrid model of LSTM & GRU

Input: Data Set of SIoT network N nodes of different features.

Output: Classified trusted and untrusted node

Step 1: Define the SIoT network nodes with different object features.

In flow centrality

$$D_{in}(P_i) = \left|P_{ji} \in P\right|, j \neq i$$

$'P_{ji}'$is the link between the node.

Out flow

$$D_{ot}(P_i) = \left|P_{ij} \in P\right|, i \neq j$$

$'P_{ij}'$is the link between nodes.

Step 2: Compiling the Data set for model processing with efficient Optimization.

$$D_B(P_i) = \sum_{P_s \neq P_i \neq P_d} \frac{\mu_{P_s,P_d}(P_i)}{\mu_{P_s,P_d}}$$

$$D_c(P_i) = \frac{N}{\sum_{Py} d(P_y,P_i)}$$

Where N is the number of vertices in the network and d (Py, Pi) is a distance between vertices Py and Pi.

Step 3: Trust classification fitting is verified for the neural network model

$$E_v(P_i) = {}^{1}/_{d}\, \alpha \sum_k \gamma_{P_k,P_i} * E_v(P_k)$$

Where A=$\alpha(k,i)$ is the adjacency matrix of a graph and γ a constant

Step 4. Evaluation and validation for SIoT Network Trust classification

$$R_p(P_i) = \rho \sum_k \frac{A_{P_k,P_i}}{d_k} * R_p(P_k) + \beta$$

where ρ and β are constants and dk is the out-degree of node p_k if such degree is positive, or d_k = 1 if the out-degree of node p_k is null. Again, A = (ai,j) is the adjacency matrix of a graph.where A=$\alpha(k,i)$ is adjacent matrix.

Step 5. Trust classification and Predictions with optimizations.

$$\mathrm{H_c(P_i)} = \beta \sum_{\mathrm{k}} \gamma_{\mathrm{P_i,P_k}} * R_p(P_i)$$

where A = (ai,j) is the adjacency matrix of a graph and $R_p(P_i)$ is the Page Rank of the node which is given by , β is a constant

$C_c = 2Mp_i/K_i\ (K_i\text{-}1)$

$Tk = Rt(P(j,i) - TtP_{(i,j)}/N$

IV. RESULTS ANALYSIS AND DISCUSSIONS

To validate the proposed framework's efficacy, experiments were conducted using available datasets to assess the accuracy of the models. The experimental setup utilized a computer configuration consisting of an i5 CPU (Eighth Generation) with 16GB RAM, a 2TB Hard Disk, and an 8 GB NVIDIA GPU. These hyperparameters were meticulously chosen to optimize the performance of the proposed algorithm in processing SIoT datasets. The experiments were conducted using a substantial amount of training and testing data, with multiple epochs to ensure comprehensive learning. The specified batch size, learning rate, and activation functions were selected to facilitate efficient optimization during training. The processing time for the experiments ranged from 14 to 16 hours, reflecting the computational complexity of the tasks involved. Additionally, the inclusion of dropout regularization (ELM_Dropout) with a dropout rate of 0.3 helped prevent overfitting and improve generalization performance. This comprehensive experimental setup enabled thorough evaluation of the proposed framework's performance metrics, ensuring robustness and reliability in handling SIoT datasets.

The fig depicts in 4,5,6 and 7 shows the comparative analysis between the performance of the proposed model and the other learning models.

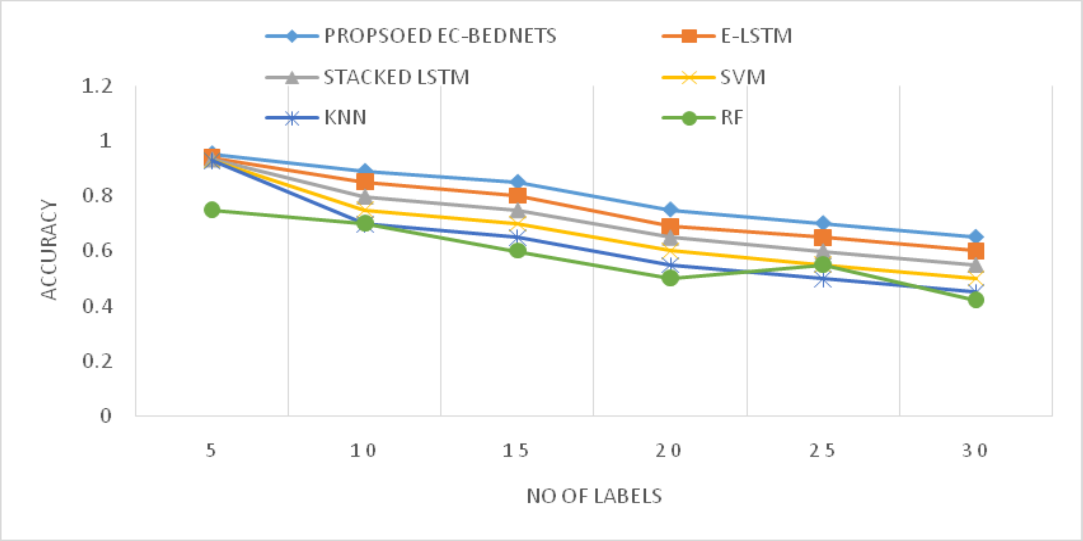

Figure 4: Proposed system accuracy at interval1

Figure 3, 4, and 5 illustrate the results of all three analyses conducted. The proposed algorithms consistently maintain high accuracy levels, ranging from 0.95 to 0.94, even as the rates of untrusted entities increase. This demonstrates the effectiveness of the boosting ensemble characteristics implemented in LSTM. In contrast, other existing models exhibit declining performance under similar conditions:

E-LSTM: Accuracy drops from 0.9 to 0.8.

Stacked LSTM: Accuracy decreases from 0.85 to 0.8.

SVM: Accuracy declines from 0.85 to 0.79.

KNN: Accuracy decreases from 0.75 to 0.68.

RF: Accuracy drops from 0.65 to 0.58.

This comparison highlights the superior performance of the proposed technique, particularly in handling increased rates of untrusted entities. To further validate the performance of our approach, we conducted comparisons with other learning models, particularly in integrating more labels and infection rates. These comparisons affirm the robustness and efficacy of our proposed system in handling diverse scenarios and outperforming existing models.

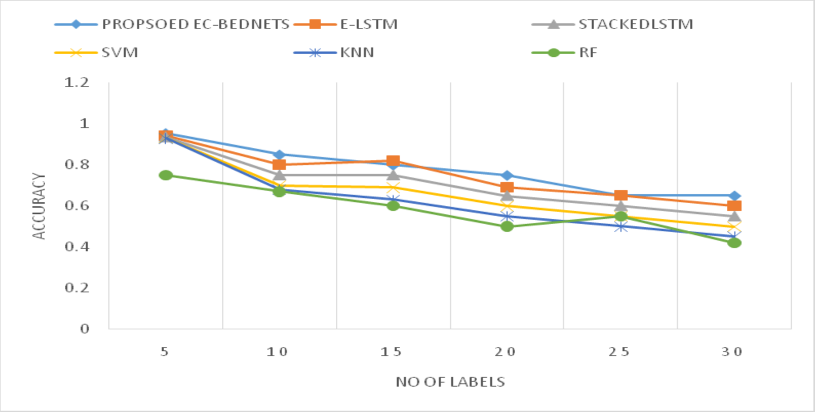

Figure 5: Proposed system accuracy at interval2

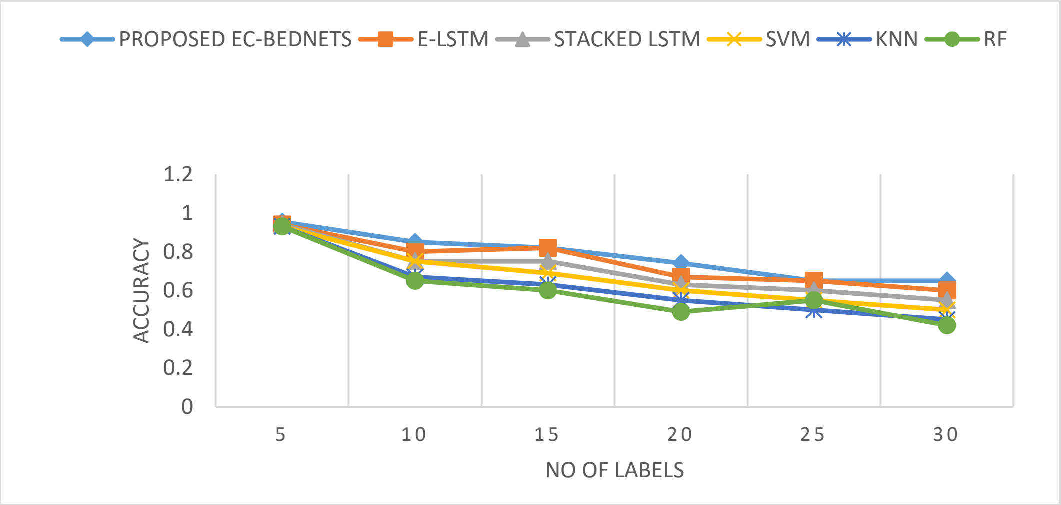

Figure 6: Proposed system accuracy at interval3

Figures 3, 4, and 5 depict the validation analysis of various learning models against different benchmarks at a high infection rate greater than 0.5 but equal to 1 (with a random value set to 0.8). In this validation, larger edge networks and social networks were utilized. The accuracy of predicting influential nodes in these networks ranged consistently from 0.95 to 0.94 for our proposed algorithms. In contrast, other algorithms exhibited greater disparities in accuracy rates when confronted with higher-order infection rates and random increase in labels.

This robust maintenance of accuracy in predicting influential nodes, even under challenging conditions such as higher infection rates and increased label randomness, underscores the efficacy of our proposed algorithms. The comparative analysis further highlights the superior performance of our approach in handling complex network scenarios, particularly in accurately identifying influential nodes within larger edge and social networks.

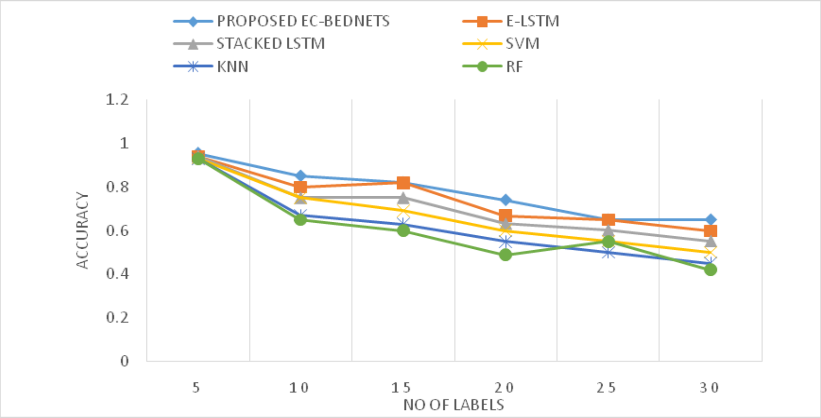

Figure 7: Proposed system accuracy at interval4

From the analysis of figures 3, 4, 5, and 6, several observations can be made: When the labels are sparse, accompanied by a high untrusted rate (0.8), both the proposed algorithms and other learning models exhibit relatively stable characteristics with minimal variations. Specifically:

Proposed algorithms achieve an accuracy of 0.95.

E-LSTM achieves an accuracy of 0.88.

Stacked LSTM achieves an accuracy of 0.85.

Other machine learning models range from 0.80 to 0.75 in accuracy.

As the number of labels increase, the proposed framework demonstrates lesser deviations in accuracy (0.95 to 0.94), while other algorithms exhibit larger deviations. The inclusion of enhanced centrality and boosted structure in deep learning models has consistently shown superior performance in predicting influential nodes across all testing and validation scenarios. Additionally, it's important to note the characteristics of the original LSTM model and the stacked LSTM:

The original LSTM model consists of a single hidden LSTM layer with GRU, followed by a standard feed forward output layer. The stacked LSTM model extends this architecture by incorporating multiple hidden LSTM layers, with each layer containing multiple memory cells. These observations highlight the effectiveness of incorporating enhanced centrality and boosted structure in deep learning models, particularly in scenarios with sparse labels and high untrusted rates. Moreover, the stacked LSTM architecture proves beneficial in capturing complex relationships within the data, leading to improved predictive performance.

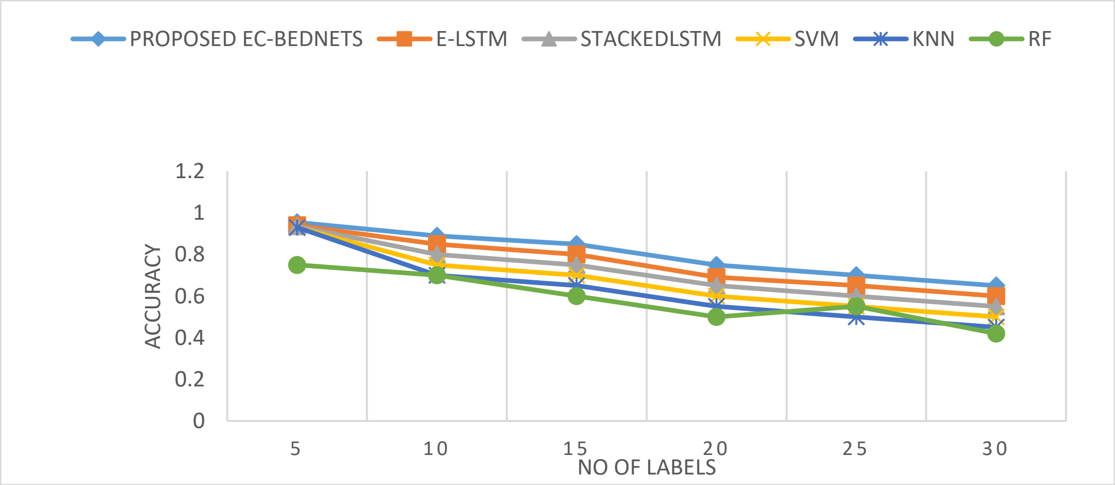

Figure 8: Proposed system accuracy at interval5

In all the figures presented above, the proposed framework utilizes enhanced centrality methods to construct diverse feature vectors, enabling the reflection of both functional and structural aspects of node locations within SIoT networks. These feature vectors facilitate the categorization of nodes based on various measurements. Subsequently, the proposed boosted deep learning framework is employed to effectively classify and rank nodes as either trust or untrusted with higher accuracy compared to existing models.

The proposed model is compared with different algorithms such as Random Forest, Support Vector Machine (SVM), and K-Nearest Neighbors (KNN). Through these comparisons, the superiority of the proposed framework is demonstrated in terms of its ability to accurately classify and rank influential nodes within SIoT networks. This comparison underscores the effectiveness of leveraging enhanced centrality methods and boosted deep learning techniques in enhancing trust evaluation and node classification processes in SIoT environments.

Overall, the proposed framework showcases significant advancements in trust management and node classification within SIoT networks, offering improved accuracy and efficiency compared to traditional algorithms. The proposed work utilizes specific parameters based on trust metrics and SIoT object relationships, resulting in an impressive accuracy of 97% across all trust metrics and SIoT relationships. This performance significantly outperforms existing models, maintaining a high accuracy of 0.97 even with increasing rates of untrusted entities. The boosting ensemble characteristics implemented in LSTM demonstrate clear advantages over other existing models, which exhibit decaying performance as the untrusted rates increase.

Comparatively, E-LSTM achieves an accuracy of 0.9 to 0.8, Stacked LSTM achieves 0.85 to 0.8, SVM achieves 0.85 to 0.79, KNN achieves 0.75 to 0.68, and RF achieves 0.65 to 0.58. These results underscore the efficiency and effectiveness of the proposed system in designing an intelligent trust classification system suitable for establishing trusted SIoT network communication with a remarkable accuracy of 97%.

Future research endeavors will focus on enhancing results further by employing more efficient learning models to predict reliable trust models based on heterogeneous devices, different services, and various objects within an SIoT environment. This ongoing exploration aims to continuously improve the robustness and reliability of trust management systems in complex and dynamic SIoT networks.

The proposed system demonstrates the utilization of various features and their significance in the context of SIoT networks, particularly based on the SIoT dataset of ADVOGATO Network Data Statistics. In this dataset, each point represents a node (vertex) in the graph, and a subset of interesting nodes may be selected for visualization of their properties across all node-level statistics. The features play a crucial role in understanding the structural and functional characteristics of nodes within the SIoT network.

The features provide valuable insights into the structural and functional characteristics of nodes within the SIoT network, aiding in the analysis, visualization, and understanding of network dynamics and behavior. By leveraging these features, the proposed system can effectively identify influential nodes, detect network anomalies, and improve trust classification in SIoT environments.

V. CONCLUSION AND FUTURE WORK

The recent advancements in Internet of Things (IoT) have paved the way for the emergence of the Social Internet of Things (SIoT), which represents a powerful amalgamation of social networking features with IoT objects. In SIoT networks, IoT objects are enabled to establish social connections with each other, forming interconnected networks characterized by object-object interactions, social relationships, reliable recommendations, and a focus on establishing trustworthy connections. Consequently, the development of an Intelligent Trust Model Identification System (ITMIS) is crucial for SIoT networks to identify misbehaving objects and select only reliable, credible, and trustworthy objects before relying on the services they provide.

However, existing frameworks often rely on conventional approaches based on linear relationships between inputs and outputs, which may result in a high misclassification ratio and invalid interpretation of user information. To address this challenge, this paper proposes a novel ITMIS that integrates non-linear centralities relationships with powerful Extreme Feed Forward Neural Networks (EFFNN), incorporating Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU). The proposed model captures key trust metrics based on centrality measurements and utilizes EFFNN, LSTM, and GRU to classify trust and non-trust objects with enhanced accuracy compared to existing models.

Extensive experiments are conducted using real-world datasets, and various trust metrics are evaluated and compared with state-of-the-art trust learning models. The results demonstrate that the proposed model outperforms existing models, providing an effective and efficient approach for designing an intelligent trust classification system suitable for establishing trust networks in SIoT environments. Future work may involve implementing the model with different learning techniques and datasets to further validate its performance and applicability.

REFERENCES

[1] Sagar, Subhash et al. “Trust-SIoT: Towards Trustworthy Object Classification in the Social Internet of Things.” ArXiv abs/2205.03226 (2022).

[2] Magdich, Rim et al. “Context-awareness trust management model for trustworthy communications in the social Internet of Things.” Neural Computing and Applications 34 (2022): 21961 - 21986.

[3] Latif, Rabia. “ConTrust: A Novel Context-Dependent Trust Management Model in Social Internet of Things.” IEEE Access PP (2022).

[4] K, Athira et al. “Classification of Trust in Social Networks using Machine Learning Algorithms.” 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) (2022).

[5] Goswami, Chandrashekhar et al. “Implementation of a Machine Learning-based Trust Management System in Social Internet of Things.” 2022 5th International Conference on Contemporary Computing and Informatics (IC3I) (2022).

[6] Sagar, Subhash et al. “Trust Computational Heuristic for Social Internet of Things: A Machine Learning-based Approach.” ICC 2020 - 2020 IEEE International Conference on Communications (ICC) (2020).

[7] Kazia, Esmeralda. “Machine learning for False Information Detection in Social Internet of Things.” Fusion: Practice and Applications (2023)

[8] Shaji, B. et al. “A novel deep neural network based marine predator model for effective classification of big data from social Internet of Things.” Concurrency and Computation: Practice and Experience 34 (2022).

[9] Ali-Eldin, Amr M. T.. “A hybrid trust computing approach for IoT using social similarity and machine learning.” PLoS ONE 17 (2022)

[10] Magdich, Rim et al. “An efficient Trust Related Attack Detection Model based on Machine Learning for Social Internet of Things.” 2021 International Wireless Communications and Mobile Computing (IWCMC) (2021).

[11] Ortiz, M., Hussein, D., Park, S., Han, S. N., & Crespi, N. (2014). The cluster between Internet of Things and social networks: Review and research challenges. IEEE Internet Things.

[12] Luigi Atzori, Antonio Iera, Giacomo Morabito, Michele Nitti, The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization, July 18, 2012

[13] J. Senthil Kumar, G. Sivasankar and S. Selva Nidhyananthan, An Artificial Intelligence Approach for Enhancing Trust Between Social IoT Devices in a Network, Springer Nature Switzerland AG 2020.

[14] Michele Nitti, Roberto Girau, Luigi Atzori, Antonio Iera, and Giacomo Morabito, A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things , 23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 2012.

[15] Chen, I. R., Bao, F., & Guo, J. (2016). Trust-based service management for social Internet of Things systems. IEEE Transactions on Dependable and Secure Computing, 13(99), 1-1. https://doi.org/10.1109/TDSC.2015.2420552

[16] Truong, N. B., Um, T. W., & Lee, G. M. (2016). A reputation and knowledge-based trust service platform for trustworthy social internet of things. Innovations in Clouds, Internet and Networks (ICIN), Paris, France.

[17] Xiao, H., Sidhu, N., & Christianson, B. (2015). Guarantor and reputation-based trust model for social internet of things. International Wireless Communications and Mobile Computing Conference (IWCMC 2015), 600-605. https://doi.org/10.1109/IWCMC.2015.7289151.

[18] Lin, Z. & Dong, L. (2018). Clarifying trust in social Internet of Things. IEEE Transactions on Knowledge and Data Engineering, 30(2). https://doi.org/10.1109/TKDE.2017.2762678.

[19] Michele Nitti, Roberto Girau, Luigi Atzori, Trustworthiness Management in the Social Internet of Things, IEEE Transactions on Knowledge and Data Engineering • May 2014.

[20] Xia, H., Xiao, F., Zhang, S., Hu, C., & Cheng, X. (2019). Trustworthiness inference framework in the social internet of things: A context aware approach. IEEE Infocom 2019 - IEEE Conference on Computer Communications, 838-846. https://doi.org/10.1109/INFOCOM.2019.8737491.

[21] Truong, N. B., Lee, H., Askwith, B., & Lee, G. M. (2017). Toward a trust evaluation mechanism Decentralized Self-enforcing Trust Management System for Social Internet of Things in the Social Internet of Things. Sensors 17(6). https://doi.org/10.3390/s17061346.

[22] Chen, Z., Ling, R., Huang, C.-M., & Zhu, X. (2016). A scheme of access service recommendation for the Social Internet of Things. Int. J. Commun. Syst. 29(4). https://doi.org/10.1002/dac.2930.

[23] Abderrahim, O. B., Elhdhili, M. H., & Saidane, L. (2017). TMCoI-SIOT: A trust management system based on communities of interest for the Social Internet of Things. Wireless Communications and Mobile Computing Conference, IWCMC 2017, IEEE, 747-752. https://doi.org/10.1109/IWCMC.2017.7986378.

[24] S Abdulwahab Aljubairy, Wei Emma Zhang, Quan Z. Sheng, and Ahoud Alhazmi " SIoTPredict: A Framework for Predicting Relationships in the Social Internet of Things". Springer Nature Switzerland AG 2020, CAiSE, LNCS 12127, pp. 101–116, 2020.

[25] Chethan Raj C et.al, "Trust Evaluation Model for SIoT Using Resilient Approach", JATIT, 15th September 2023. Vol.101. No 17, ISSN: 1992-8645, E-ISSN: 1817-3195, www.jatit.org, © 2023 Little Lion Scientific.

[26] Chethan Raj C et.al "Trusted Communication using objects Semantic Behavioral analysis for Social internet of things" International Conference on Recent Research Advancements in Computational Sciences ICRRACS-2023 Dec 1-2, 2023.

[27] Chethan Raj C et.al "Trusted Device analysis and classification model for Social internet of things" International Conference on advanced Research in Engineering & Technology, ARET Feb 24, 25-2024.