IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 11, Issue 4, Dec 2023

TOWARDS A MACHINE LEARNING-DRIVEN TRUST EVALUATION MODEL FOR SOCIAL INTERNET OF THINGS: A TIME-AWARE APPROACH

M ANUSHA[1], MANTIPALLY SAI RAJU[2], MINPUR SHIRISHA[3], PURIMETLA RAMANI[4], MOHAMMED

[2,3,4,5] UG Students, Dept of CSE, MALLA REDDY INSTITUTE OF ENGINEERING AND TECHNOLOGY(AUTONOMOUS), Dhulapally, Secundrabad, Hyderabad, Telangana, India.

ABSTRACT:

Social Internet of Things is a trend in the technology which allows to the add objects to the network through which communication is possible using unique object relationship and ability to transfer the data in a network. Internet of Things is able to achieve more efficiency in decision making, Social internet of things is a subset of Internet of Things that establishes the relationship with other objects for effective communication and can improve the scalability, trust, resource management using social trust computing. Many existing models are not dynamic in nature in proving the trust with objects and user interaction and decision making process is not identifiable, the proposed Resilient Based Social Internet of Things model increases performance of evaluation with various attributes like information gain, resilience of the system, cooperativeness and trustworthiness. In SIoT trustworthiness is very important in defining reliability in user communications and interactions. The proposed experiments shows the significant improvement in the trust model for the AppClassNet data set and social internet of things data set in order to segregate trust and untrusts effectively in the network model with 92% information gain and high resilience by comparing with existing model.

Keywords: Block chain, bitcoin, virtual ledger.

1. INTRODUCTION:

Social Internet of Things (SIoT) is very trend in the technology act as a network connects many devices to the internet. These associated with sensors and actuators monitors human aspects by

ISSN 2347–3657
Volume 11, Issue 4, Dec 2023

supporting many applications to serve the requirements. Internet of Things (IoT) best use is to create network of resources as social and to find the social relationship to solve the particular task. The combination of IoT and social networks provides different interactions between the number objects across the network. A object with other object exhibits many forms of relationship as direct relationship, Indirect relationship also referred as direct trust and indirect trust obtaining in a network during these mutual interaction of objects across other object opens many challenges to address as risk if security and identity of the message communication. Trust in these networks is the basis for interactions between nodes or objects. Here one object will trust other objects that represent the confidence to handle the task

Assistant Professor, Dept of CSE, MALLA REDDY INSTITUTE OF ENGINEERING AND TECHNOLOGY(AUTONOMOUS),Dhulapally,Secundrabad, Hyderabad, Telangana, India.

in specific amount of time, score of trust in the form of direct or in direct is combined to make final evaluation. Many trust evaluation modes are proposed but those failed to perform in a dynamic SIoT environment, proposed RBSIoT model shows significant improvement in building a trust in a network with independent node interactions using attributes like Resilience, Information gain, Cooperativeness with machine learning approach [21]. As SIoT is a subset of Internet of Things (IoT) that establishes the relationship with other objects for effective communication and the trust with objects and user interaction and decision making process is not identifiable for an dynamic environment, the proposed Resilient Based Social Internet of Things (RBSIoT) model increases performance of evaluation with various attributes like information gain, resilience of the system, cooperativeness and trustworthiness. Trustworthiness is very important in defining reliability in user communications and interactions. The proposed experiments shows the significant improvement in the trust model for the AppClassNet data set and SIoT data set in order to segregate trust and untrusts effectively in the network model with 90% information gain and high resilience by comparing with existing model. Resilience in a social network

is to provide the structure to operate continuously without affecting functionality, able to perform even under improper functionality to meet rapid and dynamic requirements. In community it is the

ISSN 2347–3657
Volume 11, Issue 4, Dec 2023

responsibility of the network to support each other to know about risks, supporting between objects to promise the response time, recoverability, authenticity, connectedness and perseverance in the network. Information gain is related to nodes presence during the ommunication across with other nodes when doing actions, gives complete information whether a node is contributing in effective communication in the network. Availability of a system is directly relying on the activity of the nodes. Sometimes if a node is responding in a network then percentage of information gain becomes less to the particular nodes and also helps the system to recover and replace the nodes with some other nodes as given by the authority.

2. LITERATURE SURVEY

IoT with social concept has trend in the market to get the insight of data where data from different sources collected in data store then it is segregated according to feature set of data in order to reduce the dimensionality of data. Once the dimensionality reduced then the main focus is on subset of data which leads to fast trust evaluation can be build, many approaches proposed and existed which unable to calculate trust in the network to achieve most reliable and available network proposed system is implemented with resilient system to make system always up in evaluating trust in a network using cluster coefficient, centrality, proximity, betweenness. Using algorithm and experiments proved that system is comparatively improved in the evaluation of trust model. Trust Communication evaluation in Social IoT by Wafa Corinne[1] described about internet of things with social network in which privacy, data integrity how to ensure these attributes in social media is considered. Trustworthiness communications and interactions also major attributes in the discussion, different types of attacks is not ensured in this work. Proposed model address this integrity of the nodes communication. Maryam Khani[2] discussed about to evaluate trustworthy model using service evaluation presently online social network model and QoS based evaluation model used in this model but these model not proved to achieve trust in the network. Honest and dishonest devices or nodes can be identifies in the network. Social IoT Object relationship in Social IoT by Michele Nitti and Roberto[3] talks about network scalability in information discovery with number of heterogeneous nodes. To identify the objects relationship to process the task in P2P peer to peer networks. Feedback system is also a part of evaluation

ISSN 2347–3657
Volume 11, Issue 4, Dec 2023

system. Malicious part of the network is explained to identify using centrality in given network.

PROPOSED SYSTEM:

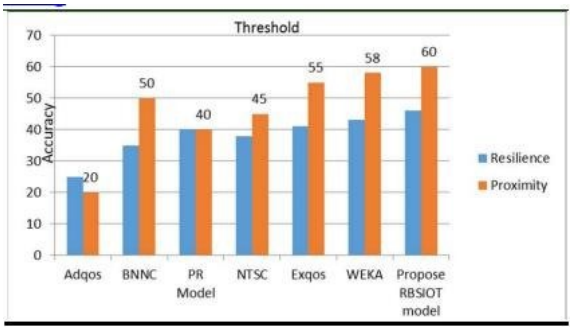
Cybersecurity, as a crucial aspect of the information society, requires significant attention. Fortunately, the concept of trust, originating from the field of sociology, has been under extensive research in order to enhance cybersecurity by evaluating the trustworthiness of nodes with artificial intelligence (AI) techniques in distributed networks (DNs). However, the scalability issues faced by AI-enabled trust hinder its integration with the DNs. Currently, there is a lack of a comprehensive review article that explores the current state of AI-enabled trust development applications. This paper aims to address this gap by providing a review of the state-of-the-art AI-enabled trust in DNs. This review focuses on the concept of trust and how it can be facilitated through AI, particularly utilizing machine learning and deep learning methods. Additionally, the paper provides a comprehensive comparison and analysis of three key domains in the field of AI-enabled trust: trust management (TM), intrusion detection system (IDS), and recommender systems (RS). Some open problems and challenges that currently exist in the field are manifested, and some suggestions for future work are presented.

3. METHODOLOGY

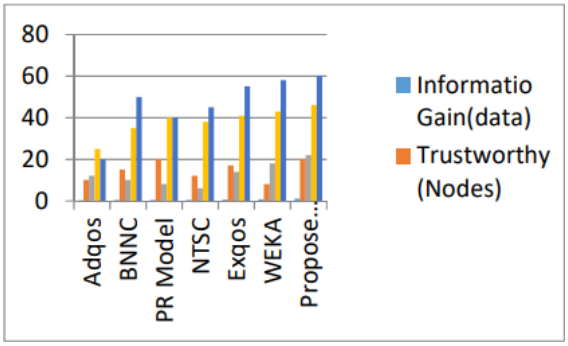
Trust in networks involves assumptions, expectations, and behaviors, making it a concept that relates to both subjective beliefs and objective reality. Drawing upon the definitions of trust in sociology and psychology, we can summarize the properties of trust in networks as follows: • Dynamicity: Trust exhibits a dynamic and changeable nature influenced by both subjective and objective factors. The level of trust between parties tends to increase as the number of successful interactions grows. Conversely, trust diminishes when interactions result in failures or negative outcomes. • Subjectivity: Trust is not solely determined by the historical behavior of the trustee, rather, it is also influenced by the subjective judgments of different trustors. These judgments can be influenced by various factors, including changes in the trustor's status or circumstances. • Hard to get, easy to lose: When an interaction fails, the decrease in trust is typically greater than the increase in trust resulting from a successful interaction. • Unequal: Due to the subjective nature of trust, the degree of trust between two entities may not be equal. It can vary depending on individual perceptions, experiences,

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 11, Issue 4, Dec 2023

and specific interactions. • Partial transferability: Trust relationships are often transferable, meaning that if node A trusts node B and node B trusts node C, it does not necessarily imply that node A trusts node C. The transferability of trust is valid only under specific conditions and cannot be assumed in all cases. • Time-decaying: The reliability of a trust value diminishes over time. When evaluating trust, the weight assigned to a trust value assessed further back in time should be lower compared to more recent trust values. By assigning a higher weight to recent evaluations, a more accurate representation of the current state of trust can be achieved. Furthermore, there are other properties of trust that have not been explicitly listed. Researchers could delve deeper into the nature of trust within social interpersonal relationships and develop definitions that align more closely with real-life expectations.



To demonstrate the significance improvement in the proposed algorithm is tested using data set, comparative methods and evaluation metrics. The data set considered is time series data set with trust feature set {Cooperativeness, Centrality, Resilience, proximity, Cluster Coefficient} employed machine learning approach used with AppClassNet commercial data set for research and this trace contains social information utilized to compute trust features. Data set has 80 nodes, 18500 interactions with 5000 pair of nodes here we used unsupervised clustering Kmean clustering algorithm.



CONCLUSION

Trust evaluation model with feature selection is used in this proposed work which reduces the data dimensionality and to focus on required relationship analysis using proximity. Cooperative objects and non cooperative objects segregation helps to build resilient social system with more dynamic functionality. Betweenness centrality and cluster coefficient evaluates the network with functional nodes and non functional nodes. System collects data from various sources will leads to privacy factors which can be addressed here in the proposed model with

ISSN 2347–3657
Volume 11, Issue 4, Dec 2023

resilience concept can make system more available with object interaction trust can be evaluated much better way compared with other works existed. Accuracy is compared with various methodologies and the given proposed method shows standard accuracy factor compared to other methods where one more method discussed with 80% resiliency achieved. Proposed methods RBSIoT model demonstrated better improvement in the trust evaluation accuracy and information gain with 0.99 Trustworthy with 20 and Cooperativeness with 22.

REFERANCES

[1] Abdelghani, Wafa et al. “Trust Evaluation Model for Attack Detection in Social Internet of Things.” Crisis (2018). Ali-Eldin, Amr M. T.. “A Cloud-Based Trust Computing Model for the Social Internet of Things.” 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC) (2021): 161-165.

[2] Al-Thanoon, N. A., Algamal, Z. Y., &Qasim, O. S. (2021). Feature selection based on a crow search algorithm for big data classification. Chemometrics and Intelligent Laboratory Systems, 212, 104288.7.4.37 (2018): 168.

[3] Abdulhamit subasi, Esrra Molah, Fatin Almkallawi, “Intelligent website detection using random forest classifier”,ICCIS, 2019.

[4] Bil Yuchen Lin, Ying Sheng, “FreeDom A Transferable Neural architecture for structured information extraction on web documents”, Pages 1092-1102, 2020..

[5] Benoit Potvin, Roger Villemaire, “Robust web data extraction based on Unsupervised visual validation”, pages 77-89, ACIIDS, 2019.

[6] Dongkyn Jeon, “Random forest algorithm for Linked data using parallel processing environment”, pages 372-380, IEICE, 2016.

[8] Gill, S. S., &Buyya, R. (2019). Bio-inspired algorithms for big data analytics: a survey, taxonomy, and open challenges. In Big data analytics for intelligent healthcare management (pp. 1-17). Academic Press.