Journal of Theoretical and Applied Information Technology

15th September 2023. Vol.101. No 17
© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

TRUST EVALUATION MODEL FOR SOCIAL INTERNET OF THINGS USING RESILIENT APPROACH

[1]CHETHAN RAJ C, [2]DR.J HANUMANTHAPPA, [3]SHARATH KUMAR G N, [4]INCHARA G P

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

[2]Professor, Department of Studies in Computer Science, University of Mysore(UoM), Mysore, India

[3]Research Scholar, Department of Studies in Computer Science, UoM, Mysore, India

[4]Research Scholar, Department of Studies in Computer Science, University of Mysore, Mysore, India

E-mail: [1]chethanraj016@gmail.com, [2]hanums_j@yahoo.com, [3]sharathkumargn@compsci.uni-mysore.ac.in@gmail.com, [4]incharainchu608@gmail.com

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: *Trust Model, Rbsiot Approach, Cluster Coefficient, Centrality, Information Gain, Cooperativeness, Betweenness*

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 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 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

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 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 communication 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. Centrality and cluster coefficient in a network also gives valuable information to find key importance of a node in executing the task or contribution of the node via tie in a network different type of centrality is used to perform context importance of the node in a network. Clustering coefficient is used in a network or a cluster to analyze dissimilarity of an object in the cluster this technique also defines robustness of the network, in this global and local cluster coefficients will be used to perform analysis of node is it properly connected to other vertices in a directed graph.

Cooperation between nodes using proper tie also defines the strength of the social IoT model data collected via various sensors and actuators are analyzed based on feature set generated and it is storing as the objects feature of the cooperative nodes in order to evaluate and analyze the trust in a given model so that trustworthiness is used properly and proposed model shows how to segregate the insight value of the object.

Flow of the paper starts with defining social internet of things approach using resilience technique followed by related work which defines detailed about methods and how data objects analyzed to make it as cooperative and non-cooperative then works followed with architecture and algorithm to define process of Internet of things with feature subset of data adapted with mathematical model to support implementation. The comparison of various attributes like cooperativeness, cluster coefficient, centrality, information gain, proximity to give how evaluation metrics help to improve trust evaluation and getting insight of data.

2. RELATED WORK

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

Trust evaluation model by Nguyen Binn [5] explains how to use trust indicators with attributes as reputation, experience and knowledge also personal experience and opinion model to build trust model Reliable and trusted model described by Subhash Sagar [6] uses machine learning driven model using friendship and community of interest as attributes. Cooperativeness of objects is used to bring back the model to segregate trusted and untrusted objects in a network. Recommendations and reputation model by Upul Jayasinghe [9] described about to build proper associations of objects with robust algorithm is proposed in distributed environments.

Trust evaluation matrices by Ting Li [10] proposed a model based on service computing using static sensor trusted device using temporal and quality factors. Local and global evaluation process is used to prove the data trustworthiness and service trustworthiness with high percentile.

Preference based trust evaluation model by Uthpala [13] build by operational abilities of objects and to compute the trustworthiness of the network with predefined data set. Strength of the objects and energy used to analyze which yields malicious nodes in a network.

Scope of the proposed system is mainly possible by adapting resilient approach and these system is in active processing state even if any failures happens then it recovers ad become available to the evaluation. Many existing approaches are not promising on these factors and different trust evaluation models are not effective compared with the proposed system architecture. The layered approach shown above also incorporate different trust evaluation methods for different context hence system act as dynamic system.

3. TRUST EVALUATION ARCHITECTURE

In figure 1 the architecture of trust model is described in detail, here the data sources is generated from various intelligent device, sensors, actuators, laptops, machines and embedded systems. In the social IoT, crowdsourcing expands the way for numerous of data-based applications reaching data successfully such applications provide timely and convenient services for users in the recent years. For instance, the health service has enabled the citizens to provide timely treatment that was previously inaccessible. Traffic service has provided citizens with appropriate travel routes, recommendations and traffic jam information by computing a large amount of traffic flow data. Undoubtedly, the trustworthy of such data-based services is based on the trustworthy of original data from the trusted devices based on object relationship. In the social IoT, a person wearing smart devices such as tablet, smartphone, and smart band, etc. [28] can act two roles, i.e., a data provider and a service requester respectively. A data provider conveniently senses surrounding data and report it to cloud server that generates and processes various kinds of services [29]. Meanwhile, a service requester can enjoy variety of social services through service recommendation [30]. Therefore, enhancing data trustworthy [31, 32] is significant and challenging issue for generating trustworthy services in the social IoT, which highlights the need to develop appropriate schemes to tackle such issue is required.

Generated data is stored in a data center instead of selecting the entire data set from date center here feature selection model help us to take required feature data from the base. Feature data set from the data is obtained after obtaining these data verified with attributes of proposed model.

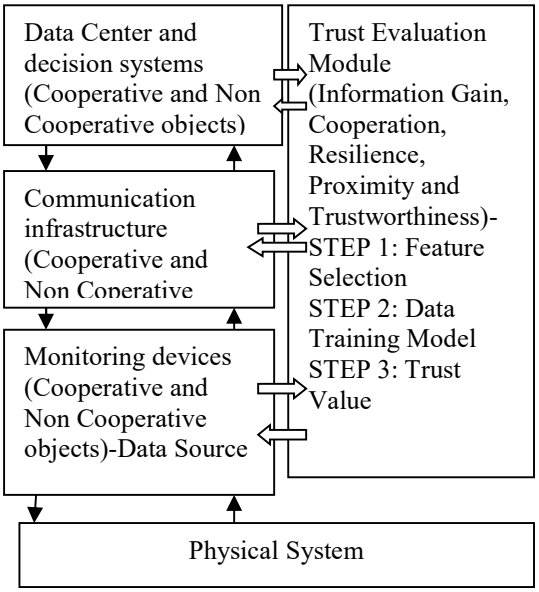

Figure 1. Architecture of Trust Evaluation Model and Object Segregation

Information gain, cooperativeness, resilience, proximity, centrality and trustworthiness are different parameters used to analyze the trust in a social network these parameters much influence the trust in network. Information gain take away the features in the data set with optimization by collecting the information about features can analyze the interaction communication with other nodes or across the nodes in network. Relation between the things as objects, events and individuals to segregates the related features

thereby reduces the dimensionality of the data set of each object in the context.

To make betterment in the social interaction and maintaining the relationship across the objects with well-connected ties through this social network is able to recover and respond from any type of failures in the system. Proximity is another attribute help in clustering or to make a network with more direct relationships with how objects interacts, responds and interpret the system with friendship. Object association with other object in a network closely defines the proper relationship.

In the Figure 2 diagram its clearly describes the relationship between the objects such as sensors, actuators, laptops and Embedded systems each one is considered as objects based on the interaction between the set of objects relationship is classified as SOR (social object relationship), GSTOR (Guest object relationship), POR (Parental object relationship), SIBOR (sibling object relationship), CLOR (Co-location object relationship). In set of devices one node act as parent, child or siblings based on this interaction and structure is showed in the diagram.

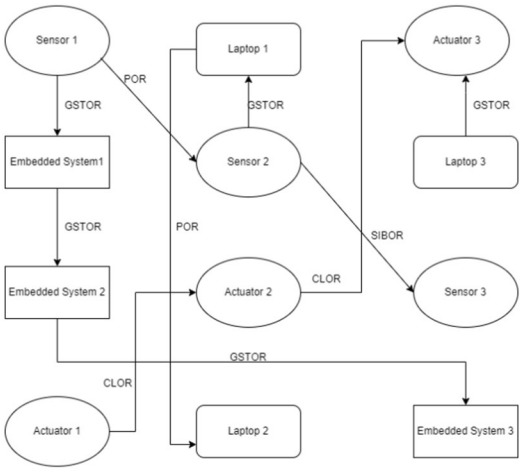

Figure 2. Parent Object Relationship Model

Embedded system objects can be laptops, digital gadgets and sensors are this devices are consider in order to collect the data for transmission of data across the nodes. The data collection is done by different sensors and actuators associated with to take action to perform in the object relation network. The object laptop is a computing device accepts data from sensor object and actuator object in which embedded system is used to execute the application and to process the output.

Each object associated with principle components as data, control and trust evaluation by acting as either parent node, child node or sibling node. Data is collected from the various objects as gain of information, about the status of the node and its interaction with its own nodes or with other nodes. Object will control the cooperativeness of the neighbor nodes to build the evaluation in the model and trust is basically evaluated with resiliency in the social network to improve the trustworthiness. Each tie in the network and nodes as to measure with proximity and is act as main attribute to build the association and to improve the effectiveness of trust.

The layered architecture of trust model is implemented to represent how data is received as sample data and collected from multiple sources used to manipulate and analyze representative subset of data objects and to find data patterns, which classified into trained data of data set to subset of feature model. Data is trained to understand how to apply technologies and to make decisions.

Then feature selection [10] is used to transform raw data collected as inputs to the model then that data is required to some algorithms. This process reduce the number of features by creating new features from existing data which helps to reduce set of features, data applied to select predictors to split data using best predictors so that estimate errors by applying tree to data if not true repeat until stop tree growth is fulfilled. Data scraping performed to make data feasible, After estimation with proximity if it as expected go to next until specified number of iteration to obtained. Sample data and estimation process is correlated with each other and feature selection of predictors is related to each other objects.

Network interaction layer is responsible for handling social evaluation for different types of data using unique protocols and to train the model and e-model for the data set generated with different protocols as protocol is different data generated is also in different way. Data objects is trained well to perform evaluation of trust using popular models like coefficient and centrality factors of each object as relation. Fifth layer is data structure layer which is capable of addressing types of data as structured, unstructured and semi structures some data is of big data there to find the core value of the data to be selected for the evaluation of trust between the objects once the proper trust value is generated then it is accessible via application interfaces in the network to see the communication collaboration and relationship establishment between the nodes using suitable ties all over.

4. MATHEMATICAL MODEL

In this section, equations related to proposed model for the entropy is divided to have features set related with mentioned attributes sample variance with standard deviation and sample data sets are presented. In this approach, n indicates data entries for the mean when working with population data sets, population data contains all members of the data set, such as a part, subset, or solution by deciding whether to proceed with a sample or the entire population.

In the below equation (1), K-mean clustering is used to partition many objects into k-clusters. Every object belongs to the nearest mean of a cluster. This method produces different clusters with distinction. Using the priori concept, computation is performed to minimize total variance and the squad error function. Information gain of each objects as relation which is able to collect the information to tabulate the gain from entropy attributes. Different object relationship used to explore the trust evaluation and to measure the effectiveness.

$$Gain = E(p) - \sum_{i=1}^{k} \frac{\text{ni}}{\text{n}} \text{E(i)} \quad \ldots\ldots\ldots\ldots (1)$$

In equation (2), the data set has all other relevant data with a specific feature set with all possible values. Sampling is always part or subset of available data. n is number of iterations with probability or category and C_i is the i^{th} category, P(Ct)) probability of the i^{th} category are all the subsets of data taken with their mean. $P(C_i|t)$ conditional probability of i^{th} category given and appeared.

$$IG(t) = \sum_{i=1}^{m} P(Ci)logP(Ci) + P(t)\sum_{i=1}^{m} P(Ci)|t)logP(Ci|t) + P(\bar{t})\sum_{i=1}^{m} P(Ci)|\bar{t})logP(Ci|\bar{t}) \quad \ldots\ldots\ldots (2)$$

In the below expression (3), average of local value C_i is calculated where n is the number of nodes in network. Node i which has n_i neighbors, cluster coefficient C_i is the ratio of e_i connected pairs to number of possible connections among the N_i neighbor.

$$C = \frac{1}{n}\sum_{i=1}^{n} C_i \ldots\ldots\ldots\ldots\ldots (3)$$

Furthermore, the associated relationship information in described in the algorithm. In equation (4) and (5) supports this resilience concept, the data sampling size with the original strength of the tie σ_y^2 data set, where U is modulus of resilience [Pa] E is the modulus of elasticity. In the below equation every data generated from different objects in which objects is from smartphone as x and another object laptop is sending data across the network with all types of different relation type in the entropy.

$$U = \frac{\sigma^2 V}{2E} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

In the below equation (5), the data set is split into different attributes and entropy is calculated from the split data with σ attributes are calculated to find the probability of entropies with extension. The resultant set is obtained with product to features. Each device in the data set is an object and can communicate easily with the existence link between the objects with proper object relationship association.

$$Ur = \frac{\sigma_y^2}{2E} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Parental object relation of AppClassNet data set and SIoT data set are the main resources of data interaction to prove the efficiency of various wrapper functions and associated time is very high. Each time, according to the training mode as wrapper functions change. The time taken to validate the information using random functions in many models does not allow for the desired selection. It is dynamic in nature, as observed in the above equation. So for each model, the wrapper function is different.

Criterion on data set is considered as below equation with set of computing devices with data collection and sending proper signal to process to see the result in the visualization form

$$Ur = \frac{1}{2}\sigma_x \in_y \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

$$E(U_r) = \frac{\sigma^y}{\sigma^y}\left(\frac{1}{2}\right)\frac{\sigma_y^2}{E} \ldots\ldots\ldots\ldots (7)$$

5. RELATIONSHIP BETWEENNESS BETWEENESS ALGORITHM FOR TRUST EVALUATION MODEL

In the proposed approach, trust evaluation is analyzed using the following algorithm is described below

5.1 Cluster Coefficient Algorithm

Identifying critical nodes is very important in optimizing network structure and increasing network robustness node betweenness is also added.

Critical nodes play an vital role in applications, such as information transmission in complex networks, accurate identification of a node in networks depends on local and global network quality. Location information of nodes and information of neighbor nodes is used with cluster coefficient and betweeness of nodes.

Input: Adjacency matrix A=(aij)NxN of a network G with N nodes
Output: Order S of node i
Step 1: S=∅
Step 2: If any nodes is not calculated exits in network do
Step 3: for i from 1 to N do
Step 4: Calculate number Ti of triangle contain node i in network by adjacency matrix A
Step 5: Find the set of shortest path in network and shortest path passing through Node i by Floyd algorithm
Step 6: For j from 1 to N do
Step 7: find T(e(i,j)) of triangles contain edge e(i,j) in network by matrix A
Step 8: find shortest path σ passs through (i,j)
Step 9: End for
Step 10: Find cluster coefficient Ci of node i
Step 11: find betweenness Bi of node i
Step 12: Find general edge cluster coefficient of all edges and calculate influence factor or effectivity of node
Step 13: End For

The algorithm clearly states that the network is a randomly analyzed to find the paths between the set of nodes and best path from node i then cluster coefficient and betweenness is calculated to ensure coefficient is applicable in general to set of nodes. To find relationship between nodes and neighbor nodes is also evaluated

5.2 Information Gain Algorithm

An algorithm shown below, demonstrate how ensemble technique which ensure better performance obtained from any of the dataset and to compare two or more different analytical model and to synchronize results too increase accuracy of data retrieval methods with respect to K mean cluster is an best approach, also to increase classification[15][17] performance of a model. Every iteration verifying with multi label if the condition is holds good then fitness of data will be formulated using function fitness(). Each label is associated with unique feature [21] with data then label is added with function add (), then combination suitability is constructed if not associated then

Input: (Feature set and class label C) Population size, GenSize, N, ProbMutation Pm
Output: (S)The Best Individual in all generation
Step 1: Initialize Population as Ps*N
Step 2: Retain f1 from Fr
Ps=random primary chromosomes
for each do
Compute Fitness
end for repeat
Step 3: Select parent from population after fitness
for all new children do
retain f1 from Fr
Step 4: crossover p1,p2
Step 5: mutate end for
Step 6: Evaluate fitness
replace least fit population with new best fit
Step 7: until stopping criteria
end proc

5.3 Centrality Algorithm

In the algorithm it is very clearly specified that data is randomly trained and rechecked for reproduce with preexisted data set to get new possibilities and interaction of the nodes. Using label approach data is combined with different patterns and possible features of data set create N number of sub class objects or nodes as instance with relevance to the dataset taken build tree to resolve the efficiency and to optimize the process of trust evaluation for information. Algorithm proposed to avoid the limitations in with data lists with repetitive occurrences.

Input: G is Un weighted and Un Directed Graph
A is adjacency Matrix of network G
Output: Heat map centrality value
Step1: Calculate the farness of each node in G
Node farness =1/closeness(G)
Step2: Find the sum of farness of neighbor for each node in G
Neighbor farness=A(Node(farness))
Step3: Find average sum of farness of neighbor for each node in G
Averageneighborfarness=(neighbor farness) / Degree(G)
Step4: Calculate heatmap centrality of each node in G
HM value= Node farness-Average neighbor farness
sub_child=cross_over(p1,p2)
mutation=TRUE
mutation mut_child=mutation(p1, p2)
Step 5: To get new possibilities.
Generate sub nodes of set, as p1,p2….pn
if, here F is associated with (F1…,Ff)
do for I range from i=1 to f

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Recall to function Cross_over (p1, p2)
if ends
for ends

6. RESULTS AND DISCUSSION

In the proposed work, selection of data processing of data with resilience is the main concept in this system many equations proposed to support high availability of data objects later integrated based on the cooperativeness and non-cooperativeness.

6.1 Experimental Setup and Data set used

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 [21] 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 K-mean clustering algorithm.

AppClassNet data set and SIoT data set proposed here is used with other parameters as K value in KNN, number of variables, and maximum number of iterations to perform feature selection. The data is modeled with selected features as number of train, number of validation to increase the accuracy and to obtain data convergence and used python libraries.

6.2 Analysis of Results

Random Forest and Multi-Layer Perceptron (MLP) classifiers are also used in order to address web information extraction and make it more efficient. Fitness of attributes has been obtained for a number of iterations, as shown in section 4, which describes how algorithm yields better fitness with number of iterations, the algorithm affects fitness attributes over n number of iterations using -1 iteration values and in figure 3 elaborated to describe KNN attributes using N iterations in each case it significantly shows the improvement in obtaining information extraction as highlighted in figure 3 and 4

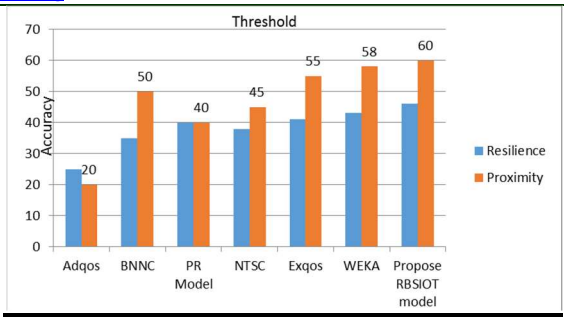

Figure 3: Performance comparison with resilience and proximity attributes.

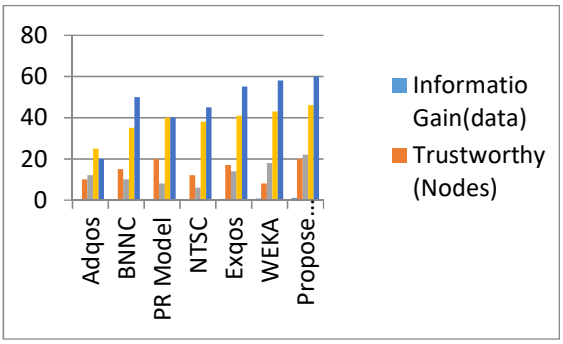

Figure 4: Performance comparison with resilience and proximity attributes.

In figure 4 above noticed that analysis of all attribute with proposed RBSIoT approach consistently shows the significance of the trust evaluation approach better and more accurate with each and every method existing shows discrepancy with many listed parameter where its maximum, so RBSIoT method will minimize system functionality and to reduce the data dimension using feature set model in network and able to evaluate with the system with all listed attributes. Centrality and cluster coefficient play vital role in making system reachable, collaborative and available to ensure effective trust evaluation and taking insight of data objects.

6.3 Comparison of Results

In Figure 5 comparison of proposed model with other approaches used in trust evaluation shows significant impact on trust obtaining and evaluation. Different metrics where information gain is analyzed to show performance of different methods. Clustering algorithm, information gain and centrality algorithm compared for attribute accuracy and flexibility in selecting required featured data when changes occur. Clustering algorithms are applied to formatted and unformatted records in data slots. If any

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

modifications in layout design are not accommodated, these shortfalls are used to generate layout designs with different patterns of the social network.

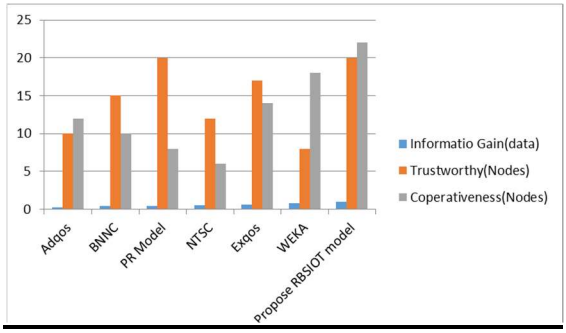

Figure 5: Comparison of approaches with different attributes.

Table 1: Comparison of methods with two attributes.

Approaches	Information Gain(data)	Trustworthy (Nodes)	Cooperativeness (Nodes)
Adqos [13]	0.25	10	12
BNNC [9] [33]	0.38	15	10
PR Model[12]	0.45	20	8
NTSC[14] [33]	0.5	12	6
Exqos[2]	0.61	17	14
WEKA[1]	0.75	8	18
Proposed RBSIoT model	0.99	20	22

Table 2: Comparison of methods with three attributes.

Approaches	Information Gain(data)	Trustworthy (Nodes)	Cooperativeness (Nodes)
Adqos [13]	0.25	10	12
BNNC [9] [33]	0.38	15	10
PR Model[12]	0.45	20	8
NTSC[14] [33]	0.5	12	6
Exqos[2]	0.61	17	14
WEKA[1]	0.75	8	18
Proposed RBSIoT model	0.99	20	22

Reference to table 1 and 2, Accuracy is compared with various methodologies and the given proposed method shows standard accuracy factor compared to other methods and also one more method discussed with 99% information gain is achieved. Proposed RBSIoT model demonstrated better improvement in the trust evaluation accuracy.

Table 3: Comparison of all methods with all attributes

a. Information Gain(data),b. Trustworthy(Nodes), c. Cooperativeness (Nodes), d. Resilience, e. Proximity					
	a.	**b.**	**c.**	**d.**	**e.**
Adqos[13]	0.25	10	12	25	20
BNNC [9] [33]	0.38	15	10	35	50
PR Model[12]	0.45	20	8	40	40
NTSC[14] [33]	0.5	12	6	38	45
Exqos[2]	0.61	17	14	41	55
WEKA[1]	0.75	8	18	43	58
Proposed RBSIoT model	0.99	20	22	46	60

Table 4: Comparison of all Approaches with dataset

Data Set	**Models /Approach**	**a. Information Gain(data),b. Trustworthy(Nodes), c. Cooperativeness (Nodes), d. Resilience, e. Proximity**				
		a.	**b.**	**c.**	**d.**	**e.**
Feature Simulation Model	Self Promoting Attacks[25]	70	40	0.50	-	0.54
Service Consume Device Data	MCTSE-Mutual Context-aware Trustworthy Service Evaluation[13]	60	30	0.60	40	-
Motion To Trace Position	Small World In Motion (SWIM)[26]	55	25	0.55	35	0.48
Jera Model	RDFS Web Technology	78	35	0.33	-	0.52
Crawdad Data Set	Reputation, Experience and Knowledge REK-Model[17]	85	36	0.25	48	0.6
Sigcomm Data Set	Time Aware Approach[27]	80	20	0.65	-	0.35
Proposed RBSIoT model	Resiliency Based	92	50	0.75	80	0.72

The study on different proposed concept is visualized in table 3 and 4, were the models on various applications as described in the table. Feature classification model works with different kinds of attack using depth first search algorithm to find trust evaluation where it yields the information gain as 70% with trustworthiness across 40 nodes but failed to achieve the resilience. Mutual context aware evaluation approach using service data set able to obtain information gain of 60% with cooperativeness is 60% here it is failed to address the proximity between nodes in the network. Similarly REK model in crawdad data set which is

network data set contain real data streams of routes information between source node and destination node around 600 sets able to obtain the resilience of 48% with proximity of about 60%.

In Sigcomm using time aware approach in social network to analyze the traffic analysis of data here this method shows significant impact on evaluation of trust evaluation with attributes in this approach also it fails to bring resilience in the network when failures occurs. Proposed model is focus on the resilience of the participating nodes in social network which able recover from the failures when occurs frequently. Information gain and cooperativeness achieved here with 92% and 75%.

Traditional systems and advanced system models use automated methods to extract information. The contents and model structure play a vital role in establishing relations between a page and page level attributes. If there are any changes in the model, then the wrapper function will enable the deployment to make the function work. Compared to our model, it's not possible to ensure the efficiency and here more complication and achieve better trust mapping across the objects.

The proposed model provides the application specific service based on the objects relationship. The proposed model facilitates the interaction between heterogeneous objects through relationships. Hence, every object in the network autonomously establishes various types of relationships and uses the resulting links to propagate in the network to avail the trusted service for different domains of applications. SIoT shares information through relationships and provides information anywhere and anytime. Moreover, it also provides trusted information by using relationship conditions.

7. 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 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.

In the proposed work a new trust-evaluation model is able to detect untrust nodes, based a reliable and resilient system. In future prospects the system is developed for trust-management mechanism based on the proposed trust-evaluation model with reference to different real time applications and this mechanism must ensure not only trust establishment based on information gain and cooperativeness but also considering the propagation, storage, and updating of trust using efficient learning model.

REFERENCES

[1] Abdelghani, Wafa et al. "Trust Evaluation Model for Attack Detection in Social Internet of Things." Crisis (2018).

[2] 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.

[3] 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.

[4] Abdulhamit subasi, Esrra Molah, Fatin Almkallawi, "Intelligent website detection using random forest classifier",ICCIS, 2019.

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

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

[7] 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.

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[9] Gutierrez, F., Dou, D., Fickas, S., et al.: A hybrid ontology-based information extraction system. J. Inf. Sci. 42(6), 798–820 (2016).

[10] Hiranandani, P., Pilli, E. S., Chand, N., Ramakrishna, C., & Gupta, M. (2018, January). Big Data Analytics Using Multi-Classifier Approach with Rhadoop. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 478-484). IEEE.

[10] Ji, B., Lu, X., Sun, G., Zhang, W., Li, J., & Xiao, Y. (2020). Bio-inspired feature selection: An improved binary particle swarm optimization approach. IEEE Access, 8, 85989-86002.

[11] Jayasinghe, Upul et al. "RpR: A Trust Computation Model for Social Internet of Things." 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld) (2016): 930-937.

[12] Jeyasingh, S., &Veluchamy, M. (2017). Modified bat algorithm for feature selection with the wisconsin diagnosis breast cancer (WDBC) dataset. Asian Pacific journal of cancer prevention: APJCP, 18(5), 1257.

[13] Khani, Maryam et al. "Context-Aware Trustworthy Service Evaluation in Social Internet of Things." International Conference on Service Oriented Computing (2018).

[14] Li, Ting et al. "NTSC: a novel trust-based service computing scheme in social internet of things." Peer-to-Peer Networking and Applications 14 (2021): 3431 - 3451.

[15] Michele Nitti, Roberto Girau, Luigi Atzori, Antonio Iera, Giacomo Morabito:A subjective model for trustworthiness evaluation in the social Internet of Things. PIMRC 2012: 18-23

[16] Nguyen Binh Truong, Hyun-Woo Lee, Bob Askwith, GyuMyoungLee: Toward a Trust Evaluation Mechanism in the Social Internet of Things. Sensors 17(6): 1346 (2017)

[17] Nguyen Binh Truong, Tai-Won Um, Bo Zhou, GyuMyoungLee: From Personal Experience to Global Reputation for Trust Evaluation in the Social Internet of Things. GLOBECOM 2017: 1-7

[18] Mohan, M. M., Augustin, S. K., &Roshni, V. K. (2015, December). A BigData approach for classification and prediction of student result using MapReduce. In 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS) (pp. 145-150). IEEE.

[19] Premarathne, UthpalaSubodhani. "MAG-SIoT: A multiplicative attributes graph model based trust computation method for social Internet of Things." 2017 IEEE International Conference on Industrial and Information Systems (ICIIS) (2017): 1-6.

[20] Premarathne, UthpalaSubodhani. "Residual Energy Aware Trust Computation Method for Social Internet of Things." 2019 14th Conference on Industrial and Information Systems (ICIIS) (2019): 470-475.

[21] Sagar, Subhash et al. "Towards a Machine Learning-driven Trust Evaluation Model for Social Internet of Things: A Time-aware Approach." MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (2020):

[22] 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): 1-6

[23] Sagar, Subhash, et al. "A time-aware similarity-based trust computational model for social internet of things." GLOBECOM 2020-2020 IEEE Global Communications Conference. IEEE, 2020.

[24] Qi, C., Zhou, Z., Sun, Y., Song, H., Hu, L., & Wang, Q. (2018). Feature selection and multiple kernel boosting framework based on PSO with mutation mechanism for hyperspectral classification. Neurocomputing, 220, 181-190.

[25] Tyagi, Himani et al. "A detailed study on trust management techniques for security and privacy in IoT: Challenges, trends, and research directions." High-Confidence Computing (2023): n. pag.

[26] Rad, Mozhgan Malekshahi et al. "Social Internet of Things: vision, challenges, and trends." Human-centric Computing and Information Sciences 10 (2020): 1-40.26

[27] Anna-Kaisa Pietilainen and Christophe Diot. CRAWDAD dataset thlab/sigcomm2009 (v. 2012-07-15). Downloaded from https://crawdad.org/thlab/sigcomm2009/20120715, 2012.

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[28] Jiang B, Huang G, Wang T, Gui J, Zhu X (2020) Trust Based Energy Efficient Data Collection With Unmanned Aerial Vehicle In Edge Network. Trans Emerg Telecommun Technol.

[29] Boukerche A, Robson E (2018) Vehicular Cloud Computing: Architectures, Applications, And Mobility. Comput Netw 135:171–189

[30] Kapetanakis S, Polatidis N, Alshammari G, Petridis M (2020) A Novel Recommendation Method Based On General Matrix Factorization And Artificial Neural Networks. Neural Comput & Applic 32(16):12327–12334

[31] Liu Y, Dong M, Ota K, Liu A (2016) Activetrust: Secure And Trustable Routing In Wireless Sensor Networks. Ieee Trans Inf Forensics Secur 11(9):2013–2027

[32] Esposito C, Ficco M, Gupta Bb (2021) Blockchain-based Authentication and Authorization for Smart City Applications. Inf Process Manag 58(2):102468.

[33] Li, Ting Et Al. "NTSC: A Novel Trust-based Service Computing Scheme In Social Internet Of Things." Peer-to-peer Networking And Applications 14 (2021): 3431 - 3451.