1. Introduction

Internet of Things is network of physical objects that contain electronics embedded within their architecture in order to communicate among each other or with external environment. The IoT facilitates integration between the physical world and computer communication networks. IoT is a very good and intelligent technique; it reduces human effort and provides easy access to physical devices. Applications such as infrastructure management and environmental monitoring require privacy and security techniques for future IoT systems. IoT also has autonomous control feature by which any device can control without any human interaction. Radio-frequency identifications, wireless sensor networks, and cloud computing are the major part of IoT systems which need to be protected. Data privacy and address security such as spoofing attacks, intrusions, DoS attacks, distributed DoS (DDoS) attacks, jamming, eavesdropping, and malware are the major issues [1]. In recent years, network attack detection has increasing interest in social networking information security. To synchronize with new or variant attacks, the detection and protection must be accomplished in a smart and effective way. Traditional attack detection methods which are not suitable for current IoT infrastructure attempt to model all kind of attacks or anomalies. However, new types of attack not even detected have already made great damages. To overcome this problem, a lot of efforts have been devoted to modeling the attack by using machine learning techniques

The aim of future IoT is to provide services for making decisions autonomously without human intervention. In this regard, trust has been recognized as a vital key for processing and handling data [2]. "Trust architecture" provides a framework that enables trusted data to flow through a service-oriented system. Different ML techniques such as decision trees, clustering, neural and Bayesian networks help any type of devices to identify patterns in different types of data sets coming from diverse sources, and take appropriate decisions on the basis of their analysis. Such challenges are faced especially in the case of embedded systems or hardware board. With the development of ML, IoT devices have to choose a defensive policy and determine the key parameters in the security protocols. As IoT devices come with restricted resources, memory and computation power, this task is challenging. ML techniques including supervised learning, unsupervised learning, and RL have been widely used to improve network security.

Many models use mathematical approach to calculate the trust value of an object regarding other objects by using the current trust and reputation values. There are several trust related frameworks used to provide privacy, reputation and social relationships. Many trust evaluating schemes have been proposed but they lack the information about generic framework details. Trust model defines all aspects of trust including information gathering, processing and producing measurable values. For feasible deployment, labeling a particular entity as trustworthy or not based on a given data set of several hundreds of interactions is a vital matter. Yet no such research found that has investigated labeling based on trustworthiness. These approaches lack generic framework in terms of application domain. Therefore, it is essential that trust mechanisms are designed and developed to look ahead to the future privacy and security where many individual objects are interconnected with new vulnerabilities. Here two-step process is followed. As the first step, a framework is proposed which defines trust metrics (TMs) under three categories: "Knowledge", "Experience", and "Reputation". It represents all parameters of trust in any application domain [3]. Then as the second step, the trust attributes (TAs) used in application area and methods which can assess them. It represents major TMs identified in application system. The focus is generating numerically measurable values by combining trust based mathematical methods with intelligent Machine Learning (ML) techniques. The method depends on a balance of several qualities of service factors like accuracy, computational resources, efficiency, and availability of data.

2. Motivation

Motivation behind work is

1. To offer understandings of trust within potential IoT applications as trust may vary according to the IoT techno-service context.
2. Traditional models of trust developed within interpersonal, organizational, and virtual and information systems contexts may be inappropriate for use within an IoT context.
3. Most existing security solutions generate a heavy Computation and communication load for IoT devices.
4. To provide computational-intensive and latency-sensitive security, especially under heavy data streams.

3. Problem Statement

To implement novel machine learning algorithm based Trust computational model for IoT services to overcome perception of uncertainty and risk before making any decisions.

4. Objectives

The objective of work is to present

1. Trust framework model which specifies the formation of trust from raw data to a final trust value.
2. Offer an analytical approach to assess the data and evaluate each individual trust feature.
3. Present a clustering algorithm to label the extracted trust features.
4. Propose an intelligent model based on a multiclass classification algorithm to combine measured TMs to formulate a trust assessment mode.

5. Literature Survey

Feng Jiang, Yunsheng Fu , B. B. Gupta,Yongsheng Liang , Seungmin Rho , Fang Lou, Fanzhi Meng and Zhihong Tian, "Deep Learning based Multi-channel intelligent attack detection for Data Security ", IEEE Transactions on Sustainable Computing, 2018.

Author proposed intelligent attack detection method consists of training and testing phase. There are three steps in training phase including data preprocessing, multi-feature extraction, multi-channel training, and also there three steps in testing phase including data preprocessing, multi-feature extraction and attack detection. The first two steps are the same in the two phases. In the training phase, data preprocessing is a combination of processing steps to provide high-quality data, including data sampling, data cleansing and data dimensionality. Multi-feature extraction is used to extract different types of data feature as vectors[2]. Multi-channel training is used to generate classifiers based on neural networks, which preserves attack features of input vectors and classify the attack from normal data. In the testing phase, after preprocessing and multi-feature extraction input vectors will be put into the multi-channel processing for classifier detection. Author introduces a voting algorithm to decide if the input test data is an attack or not. These components collaborate with each other and are optimized simultaneously to improve the accuracy of the attack detection.

Paper proposes multichannel attack detection method for information security in social networks based on deep learning. Further proposes a voting algorithm to determine whether the traffic is an attack or not, which achieves high accuracy by voting to get the majority result of the multi-channel classifiers.

Y. Wang, Y.C. Lu, I.R. Chen, J.H. Chao, A. Swami, C.T. Lu," LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks" , ICPSRT, Cambridge 2014.

In this paper, every node may exhibit social selfishness based on the social relationship with other nodes it interacts with. Every node may exhibit the number of recommendation attack behaviors: In Trustor-based recommendation attacks (TORA), a node serving as a recommender provides false recommendations about a trustee. The objective is to prevent the trustor from learning the right behavior pattern and hence decrease the trustor's decision quality[4]. Based on the notion of social selfishness, if the trustor is a friend, then it tends to speak the truth about a trustee. On the other hand, if the trustor is not a friend, then it tends to lie. A node may treat

another node as a friend, acquaintance or stranger. In Trustee-based recommendation attacks (TERA), a node serving as a recommender may perform reputation attacks on the trustee. Based on the notion of social selfishness, if the trustee node is not a friend attends to perform bad-mouthing attack to diminish the trustee node's reputation. On the other hand, if the trustee node is a friend then it tends to promote the trustee node by performing ballot-stuffing attacks. In TERA-if-TORA, a node serving as a recommender first decides whether to perform false recommendation attack based on its relationship with the trustor node. If yes, it performs bad-mouthing or ballot-stuffing attack based on its relationship with the trustee node.

It proposes regression based model which compares the variation of trustworthiness with respect to trust features in Mobile Ad hoc network (MANET). They have investigated limited number of trust features, which only represents the system level information like packet forwarding ratio, Quality of service, energy sensitivity, capability limitation and profit awareness.

W. Li, W. Meng, L.F. Kwok and H. Horace" Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model", JNCA, 2017.

The paper proposes trust management model that allows an IDS node to evaluate the trustworthiness of others based on its own knowledge and others' experience. In the framework, each IDS node can choose its collaborators according to its own experience. These nodes are associated if they have a collaborative relationship. Each node can maintain a list of their collaborated nodes, which is called partner list. This list is customizable and contains public keys of other nodes and their current trust values. The Trust Management Component is responsible for evaluating the trustworthiness of other nodes. Two types of trust: feedback-based trust and packet-based trust. The Query Component is a key component in the revised CIDN framework, which can send a set of queries to a target node[5]. More specifically, a query can contain a set of alarms while answers are alarm rankings sent back from the target node. Basically, these answers are decided by the experience, configuration and settings of each IDS node. The Collaboration Component is mainly responsible for assisting a node to evaluate the trustworthiness of others by sending out requests and challenges, and collecting the corresponding feedback. Communication component is responsible for connecting with other

IDS nodes and providing network organization and communication between different IDS nodes. To evaluate the trustworthiness of a target node, an IDS node can send a challenge to this target periodically using a random generation. When receiving the feedback from the target node, the IDS node can give a score to reflect its satisfaction level. The KNN algorithm classifies objects based on the closest training examples in the feature space. That is, an object is classified in terms of its distances to the nearest cluster. In addition, this classifier can achieve a faster speed with lower computational burden as compared to other classifiers like neural networks in the phases of both training and classification.

This paper presents trust management framework based on reinforcement learning and multiclass classification technique.

N.B. Truong, U. Jaya singhe, T w Um, G.M.Lee ,"A Survey on Trust Computation in the Internet of Things", JKICS, 2016.

Trust is defined as the belief level of an object to other objects based on direct observations and previous observations, and this belief level can be used as the consideration of taking decision in next communication process to the object. The belief level is obtained objectively through trust calculation, either directly or by previous experiences. The value of the trust calculation will be used to determine the recommendation of a trustable object. Assessment process to gain the trust value of an object can be done by calculating the trust value as a result of direct observations and the results of previous observations. Observations are generated from the object that would like to calculate the trust value, as well as from other objects which ever communicated with the object being assessed. Trust calculation is part of trust assessment, whose main purpose is to determine objectively by calculating trust value using selected algorithm or methods. The result of trust calculation usually in the form of numbers, and these numbers are modified into recommendation to decide whether an object is trustable or not[6].

Author provided survey on several trust computational schemes based on the concept of network architecture, policy, reputation and hybrid methods.

G. Yin, F.Jiang,s. Cheng,X. Li and X. He, " Autrust:A practical trust measurement for adjacent users in social network", ICCGC, 2012.

Propose a novel model aiming at solving them to calculate trust between adjacent users. Based on the real social relationships, social networks are more complicated and virtual in comparison with reality. The model extract and analyze these information which is easy to collect by API provided by social networks, including users' attributes, users' interests, relationship and interactions between users, network structure, and so on. The model consists of three dimensions which are designed as: similarity between users, familiarity between users and users' social reputation [7]. Next, the several definitions and propose the formula of the model. Lastly, how to build trust social networks. Initially all trust between adjacent users are treated equally, and for any two directly connected users in social networks, the trust we evaluate is relative, directed and asymmetric. AUTrust model can be combined with recommender systems to exert the effect of acquaintance recommender.

Author presents a computational model for trust based on similarity, information reliability and social opinions.

6. Proposed System

6.1 Generic Trust Management Framework

Trust gives decision of an object to transact with another object in an IoT ecosystem. Participating objects must take decisions based on trust value to provide/ receive services to / from objects. It is difficult to give exact trustworthiness value of an object with a high accuracy. Trustor is an object that is expected to initiate an interaction with another object and trustee as the second object that provides necessary information towards the trustor upon its request. The measurement can take either a quantitative or a qualitative form. If the trustor wants TMs in a specific format that goes with the trustor profile of interest, then the measurement can be characterized as subjective [1].Objective measurement can be described as TAs collected without any profile based filtering. It is essential to establish a generic framework which defines trust management.

Trust can be measured as task dependent, time dependent or context dependent, it is variable in nature.

6.1.1 Knowledge Trust Metric

The knowledge of TM gives direct trust evaluation; it provides a perception about a trustee before an interaction. It provides relevant data to the trustor for its assessment. If a data feature is in the form of quantities measurement, then the result is a numerical value in a certain range. TAs defines the mutual relationship between the trustor and a trustee in the form of relationship, credibility, spatial and temporal. If the trustor and the trustee are operated closely by location, relationship is based on location similarity that can be identified as co-location TA. If the two objects are in a working relationship, it is identified as co-work association. The cooperativeness under credibility represents the level of social cooperation from the trustee to the trustor[1]. The higher cooperativeness shows higher trust level in system. To track the rewarding system, history of misbehavior situations or unsuitable reactions originated by the trustee. Rewarding TA can be used to either encourage or discourage further interactions with a particular trustee based on its past character [1].

Mutuality measures the degree of profile similarity between trustee and trustor . Centrality measures the importance of trustee among other participating objects with respect to a particular task and context. The community represents whether the trustor and the trustee have a close relationship. Two objects with high community interest can interact more with each other and results in a higher trust level.

6.1.2 Experience and Reputation Trust Metrics

The experience TM is a personal observation between trustor to a trustee whereas the reputation TM reflects the global opinion of the trustee. The knowledge TM is the based on both experience and reputation. To improve the perception of the trustor, other objects can share their experience, upon a request by the trustor which can be identified as reputation or the global opinion of the trustees.

7. Computational Model

As IoT is integration of physical and logical world, it produces a large amount of data. It is difficult trustworthy evaluation process. It is important to extract trust features by scanning social and system level interaction logs and store them in a data repository for further analysis.

7.1 Co Location Relationship (CLR)

Trustor can get the required information from the selected trustee in terms of the physical location compared to other objects. The objects leaving the physical location, a decision boundary based on the distance from the trustor and the time spent within this decision boundary is considered. The objects which are within distance boundary and exceed the minimum time threshold inside the region are selected as candidate for a trustee. Once the candidates are filtered, their CL relationship with the trustor can be calculated as follows [1].

$$K_{ij}^{\mathrm{CLR}}(t) = \frac{1}{\mathbf{dist}(i,j)} \frac{\mathrm{G_i G_j}}{\|\mathrm{G_i}\| \|\mathrm{G_j}\|}$$

---------- Equation (1)

Here Gi and Gj are the GPS coordinates of the trustor i and trustee j respectively.

7.2 Co work Relationship (CWR)

In CWR, the objects which work in common IoT applications can be characterized as CWR. More focus would be on working relationship rather than their physical location. To measure CWR as a numerical value, compare the multicast interaction between a trustor and trustee a calculated below [3].

$$K_{ij}^{\mathrm{CWR}}(t) = \frac{|\mathbf{c}_{ij}^{\mathrm{MI}}|}{|\mathbf{c}_{j}^{\mathrm{MI}}|}$$

---------- Equation (2)

Where C_{ij}^{MI} is the vector of multicast interactions between trustor i and trustee j and $C_j^{MI}$is the vector of MI originated at j. $K^{CWR}_{ij}(t)$ represents a relative measurement of shared multicast messages to total messages originated at the trustee.

7.3 Cooperativeness, Frequency and Duration (CFD)

The cooperativeness TA, object should provide a trustworthy service to the trustor upon its request. The more frequent and longer the interactions among objects, the more collaboration are expected. Based on this, a numerical model for cooperativeness, frequency, and duration is derived.

Let us consider a set of interactions,c1,c2...c*n* over some period in which the trustor is interested. A trust level between trustor *i* and trustee *j* is calculated below [3]:

$$K_{ij}^{CFD}(t) = \sum_{m=1}^{n} \frac{c_m}{t_m} E(c_m)$$

----------Equation (3)

Here, n is the number of interactions indicates frequency of interaction. For the *m*th successful interaction, c*m* is the length of an interaction between the trustor and the trustee; tm is the total interaction length by the trustee. The factor c*m*/t*m* assesses the duration property, in which the trustee interacts with the trustor, relative to the total activity time of the trustee. Cm is the binary entropy function which measures the balance in the interaction or the cooperativeness which can be calculated as follows [3].

$$E(c_m) = -p \log p - (1-p)\log(1-p)$$

----------Equation (4)

Where *p* is the fraction of the interactions between the trustor and the trustee. *E*(c*m*)follows a binary distribution.

7.4 Reward System (RS)

In order to assess the historical service experiences between a trustor and a trustee needs to have a reward and punishing mechanism or a feedback model. It is always critical to

maintain the social relationships at the maximum trustworthy level and here the exponential downgrading formula shown in equation for this purpose [3].

$$K_{ij}^{\mathrm{RS}}(t) = \frac{\|C\| - \|C_{\mathrm{p}}\|}{\|C\|} e^{\left(-\frac{\|C_{\mathrm{p}}\|}{\|C\|}\right)}$$

----------Equation (5)

Here ||C|| is the total number of interactions that have taken place during a period *t*, and $||C_P||$is the total number of unsuccessful or suspicious interactions.

7.5 Mutuality and Centrality (MC)

The mutuality and the centrality TAs define the degree of similarity and importance of trustee in a social world. Higher number of mutual objects implies higher similarity. An object with a higher number of friends gets an additional advantage compared to an object that has recently joined the network. In order to avoid such circumstances, a relative measurement of mutuality compared to the total number of friends is considered [3].

$$K_{ij}^{\mathrm{MC}}(t) = \frac{|M_{ij}|}{|N_i|}$$

----------Equation (6)

Where *Mij* be the set of common friends between i and j, and *Ni* is the set of trustee's friends.

7.6 Community of Interest (COI)

The trustor and the trustee share common interest groups, is the degree of common interest or similar capabilities of the trustee compared to the trustor. Mij^{coi} as the set of communities where both the trustor and the trustee are involved in, and Nij^{coi} as the set of communities with each include the trustee as a member. The trust level of the trustee based on COI is calculated as[3].

$$K_{ij}^{\mathrm{CoI}}(t) = \frac{|M_{ij}^{\mathrm{CoI}}|}{|N_i^{\mathrm{CoI}}|}$$

----------Equation (7)

Following approach is to combine each TA through a linear equation with weighting factors as shown as

$$K_{ij}(t) = \alpha K_{ij}^{\mathrm{CLR}}(t) + \beta K_{ij}^{\mathrm{CWR}}(t) + \gamma K_{ij}^{\mathrm{CFD}}(t) + \varepsilon K_{ij}^{\mathrm{RS}}(t) + \delta K_{ij}^{\mathrm{MC}}(t) + \eta K_{ij}^{\mathrm{CoI}}(t)$$

----------Equation (8)

8. MACHINE LEARNING BASED MODEL

ML based model is proposed to analyze the TAs extracted and predict the trustworthiness of prospective transactions. In order to overcome limitation of TMs, first use an unsupervised learning algorithm to identify two different clusters or labels, namely trustworthy and untrustworthy.

Then a multiclass classification technique like support vector machine (SVM) issued to train the ML model in order to identify the best threshold level that separates trustworthy interactions from others [3]. Main objective is to differentiate malicious interactions from trustworthy interactions with maximum boundary separation and minimum outliers rather than classification itself.

8.1 Algorithm I: Clustering and Labeling

The K-means algorithm define two initial conditions first is number of clusters (*k*) second is initial centroid. Here, random assignment for initial centroid locations for a range of cluster sizes is considered. The initial inputs to the algorithm were normalized between [0, 1] in which "0" represents untrustworthiness and "1" the most trustworthiness.

To check the influence of all *n* features at once, the Principal Component Analysis (PCA) algorithm based on Singular Value Decomposition (SVD) is applied to reduce the N dimensions to two dimensions for visualization purposes [3].

The first step of the PCA algorithm is to calculate the covariance matrix that has the dimension of *n* x *n*. Secondly calculates the Eigen values and Eigen vectors. In the step two principal components *U* and *V* are calculated using the SVD function [3].

Algorithm I : Data Clustering and Labelling

Input: $\underline{X}$ **Output:** $\underline{y}$
Initialize cluster centroids $\mu_1, \mu_2, \ldots \mu_k \in \Re^n$
for k=1 to 5 do
  Repeat until convergence: {
    for i=1 to m do
      $c^{(i)}$:=arg $\min_j | |\mathbf{X}^{(i)} - \mu_k| |^2$
      μ_k:= Average of points assigned to cluster
k
    end for
  }
  $J^{(k)}(c,\mu)$:=arg $\min_k J(c,\mu)$
end for
Optimum $k \leftarrow$ Elbow method $\leftarrow$ **plot** $J^{(k)}$ vs k
for i=1 to m do
  if $c^{(i)}$ close to (0,0)
    $y^{(i)} = 0$
  elseif
    $y^{(i)} = 1$
  end if

Algorithm : Principal Component Analysis

Compute dot product matrix: $\Sigma = X^T X$
Compute eigenvectors: $[U,S,V]$=SVD$(X^T X)$
Specify the required dimension ,d: $U_d = [u_1, \ldots u_d]$
Compute d(=2) features: $Z = U_d^T X$

8.2 Algorithm II: Classification Model

The parameters having minimum error in the prediction step are chosen as the optimum factors for the SVM model. Further, it is essential to improve the accuracy of the final ML model and suppress any noise generated by the previous clustering algorithm [3]. Here, regularization techniques are used to avoid issues during the training process in Algorithm II.

Algorithm II : Classification Model

1: **Input:** $\underline{X}$, $\underline{y}$, $\underline{X}_{val}$, $\underline{y}_{val}$
2: **Output:** Weights and Decision boundary
3: //Find best parameters c and γ
4: **for** c, γ=0.01 (multiple of 3) 30 do
5: model=svmtrain(y,X,RBFK,c, γ)
6: prediction=svmpredict($\underline{y}_{val}$, $\underline{X}_{val}$,model)
7: error [c, γ]= predictions ≠ y_{val}
8: **end for**
9: **Choose** c, γ ← **minimum** [*error*]
10: [*weights*, *accuracy*, *decision values*]
11: = svmtrain(y,X,RBFK,c, γ)

Afterwards, the algorithm is trained for all the training data samples using the algorithm II and model parameters are recorded to estimate future trust values based on the incoming feature statistics.

9. Conclusion and Future Scope

In this paper, algorithm is proposed as opposed to traditional weighted summations to determine whether an incoming interaction is trustworthy. Clusters are formed based on trustworthiness. A method for labeling the data depending on their trust-worthiness is realized based on unsupervised learning techniques. Following this labeling process, a trust prediction model, which can identify the trust boundaries of any interactions and learn the best parameters to combine each TA to obtain a final trust value, is proposed based on the well-known SVM model.

References

[1] Upul Jayasinghe, Nguyen B. Truong, Gyu Myoung Lee, Tai-Won Um," RpR: A Trust Computation Model for Social Internet of Things", Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, 978-1-5090-2771-2/16 2016 IEEE pp 930-937.

[2] Feng Jiang, Yunsheng Fu , B. B. Gupta,Yongsheng Liang , Seungmin Rho , Fang Lou, Fanzhi Meng and Zhihong Tian, "Deep Learning based Multi-channel intelligent attack detection for Data Security ", IEEE Transactions on Sustainable Computing, 2377-3782 2018 IEEE pp 1-11.

[3] Upul Jayasinghe, Gyu Myoung Lee, Tai-Won Um, Qi Shi," Machine Learning based Trust Computational Model for IoT Services", IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, TSUSC-2017-10-0122 pp 1-14.

[4] Y. Wang, Y.C. Lu, I.R. Chen, J.H. Chao, A. Swami, C.T. Lu," LogitTrust: A Logit Regression-based Trust Model for Mobile Ad Hoc Networks" , in proceedings of the 6th ASE International conference on Privacy, Security, Risk and Trust Cambridge MA 2014 , pp 1-10.

[5] W. Li, W. Meng, L.F. Kwok and H. Horace" Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model", Journal of Network and Computer Applications, vol. 77, pp. 135-145, 2017.

[6] N.B. Truong, U. Jaya singhe, T w Um, G.M.Lee ,"A Survey on Trust Computation in the Internet of Things", The Journal of Korean Institute of Communications and Information Sciences (J-KICS), vol. 33, no. 2, pp. 10-27, 2016.

[7] G. Yin, F.Jiang,s. Cheng,X. Li and X. He, " Autrust:A practical trust measurement for adjacent users in social network", in Second International Conference on Cloud and Green Computing (CGC), 2012, pp. 360-367.

[8] Michele Nitti, Roberto Girau, Luigi Atzori, "Trustworthiness Management in the Social Internet of Things", IEEE Transactions on knowledge and data engineering, vol. 26, no. 5, pp. 1253-1266, 2014.