

**PCET's**

**Pimpri Chinchwad College Of Engineering  
Department of Computer Engineering**

**A Seminar Presentation  
on**

**“ Machine Learning based Trust  
Computation Model for IoT Services”**

**Presenter**

Meghana Lokhande

**Research Guide**

Dr. Dipti D. Patil

# Contents

- Abstract
- Introduction
- Motivation
- Objective
- Literature survey
- Proposed system
- References

# 1. Abstract

Large volume of sensitive information imposes many threats from the risks of data management to risk of data analytics.

To address issues, concept of trust is introduced to overcome the perception of uncertainty and risks before making any decisions.

Novel algorithm based on machine learning principles is devised to classify the extracted trust features and combine them to produce a final trust value to be used for decision making.

## 2. Introduction

- IoT introduces risks, privacy and security at both system and social level.
- Traditional privacy and security triad is not suitable for solving challenges in network.
- Aim of future IoT services is to make decision autonomously without human intervention.
- Trust computational model recognized as a vital key for processing and handling data.

# Introduction contd..

- Traditional trust evaluating schemes lack generic framework details.
- Fail to define trust for information gathering, processing.
- For feasible deployment , no labeling based on trustworthiness is investigated.
- To rectify such weakness, trust framework based on numerical approach is necessity.

### 3. Motivation

Motivation behind work is

- To offer understandings of trust within potential IoT applications
- Traditional models may be inappropriate for use within an IoT context.
- Existing security solutions generate a heavy Computation and communication load for IoT devices.
- To provide computational-intensive and latency-sensitive security, especially under heavy data streams.

## 4. Objective

This model presents

- Trust framework model which specifies the formation of trust value.
- Analytical approach to assess the data and evaluate each individual trust feature.
- Present a clustering algorithm to label the extracted trust features.
- Propose an intelligent model to combine measured TMs to formulate a trust assessment mode.

# 5. Literature Survey

Sr. No.	Paper Details	Findings
1.	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 2018.	Provide solution for privacy, security and integrity based on statistical and deep learning concept
2	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.	Presents trust management framework on reinforcement learning and multiclass classification techniques
3.	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 HocNetworks"ICPSRT, Cambridge 2014.	Propose regression model for trust worthiness in MANET and WSN



# Literature survey

Sr. No.	Paper Details	Findings
4	N.B. Truong, U. Jaya singhe, T w Um, G.M.Lee ,”A Survey on Trust Computation in the Internet of Things”, JKICS, 2016.	Proposed trust evaluation scheme based on network architecture , policy, reputation.
5	G. Yin, F.Jiang,s. Cheng,X. Li and X. He, “ Autrust:A practical trust measurement for adjacent users in social network”, ICCGC, 2012.	Presents computational model for trust based on similarity, information reliability and social opinion .

# 6. Proposed System

## 6. Generic Trust Management Framework

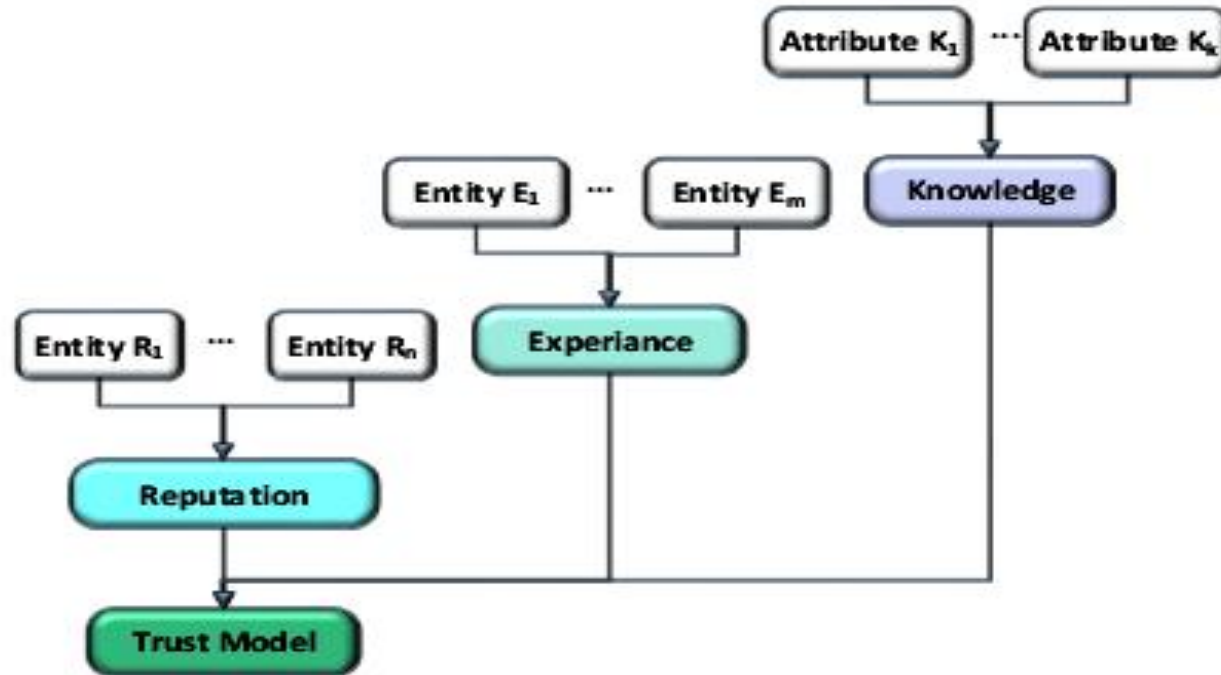


Fig. 1. A Prototype explains the trust acquisition and evaluation process based on three TMs[3]

## 6.1 Knowledge Trust Metric

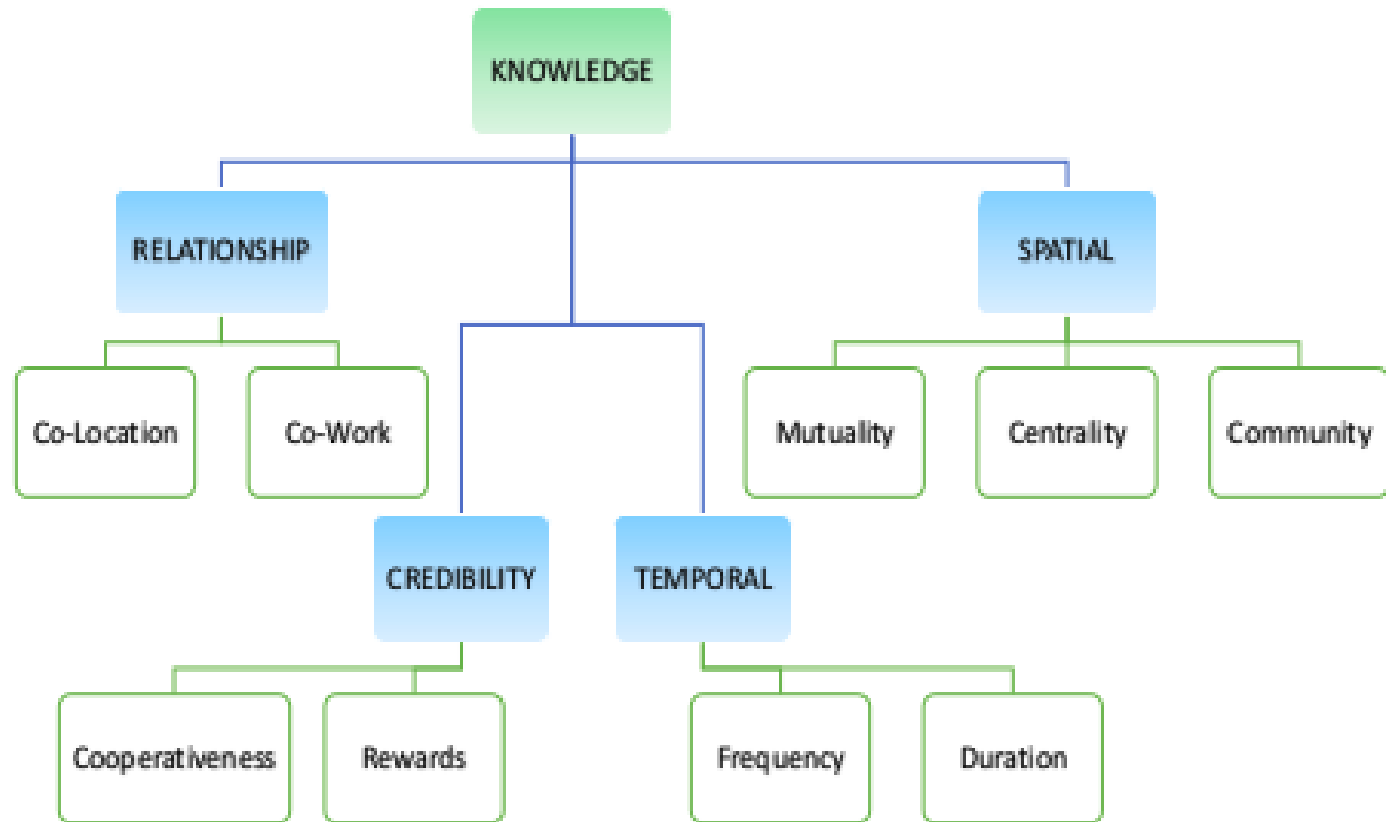


Fig. 2. Composition of Knowledge[3]

## 6.2 Experience and Reputation Trust Metrics

### Experience

- TM is a personal observation considering only interactions from a trustor.

### Reputation

- TM reflects the global opinion of the trustee
- The knowledge TM is the building block of both experience and reputation.

# 7. Computational Model

## 7.1 Co Location Relationship (CLR)

Prospective candidate for a trustee

- objects which are within distance boundary
- exceed the minimum time threshold inside the region
- Once the candidates are filtered , their CL relationship with the trustor can be calculated as follows[3].

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

where,

$G_i$  and  $G_j$  are the GPS coordinates of the trustor  $i$  and trustee  $j$

## 7.2 Co-work Relationship (CWR)

- Objects that are collaborating in common IoT applications can be characterized as CWR
- To measure CWR as a numerical value, compare the multicast interaction between a trustor and trustee[3]

$$K_{ij}^{CWR}(t) = \frac{|c_{ij}^{MI}|}{|c_j^{MI}|} \text{----- (2)}$$

Where,

$C_{ij}^{MI}$  is the vector of multicast interactions between trustor  $i$  and trustee  $j$

$C_j^{MI}$  is the vector of MI originated at  $j$ .

$K_{ij}^{CWR}(t)$  represents a relative measurement

### 7.3 Cooperativeness, Frequency and Duration (CFD)

- More collaboration from each party expected
- A trust level between trustor  $i$  and trustee  $j$  is calculated below[3]

$$K_{ij}^{\text{CFD}}(t) = \sum_{m=1}^n \frac{c_m}{t_m} E(c_m) \text{-----} (3)$$

- balance in the interaction or the cooperativeness which can be calculated as follows

$$E(c_m) = -p \log p - (1-p) \log(1-p) \text{-----} (4)$$

## 7.4 Reward System (RS)

- mechanism or a feedback model in order to assess the historical service experiences between a trustor and a trustee[3]

$$K_{ij}^{RS}(t) = \frac{\|C\| - \|C_p\|}{\|C\|} e^{\left(-\frac{\|C_p\|}{\|C\|}\right)} \text{-----} (5)$$

Where

$\|C\|$  is the total number of interactions that have taken place during a period  $t$

$\|C_p\|$  is the total number of unsuccessful or suspicious interactions



## 7.5 Mutuality and Centrality (MC)

- relative measurement of mutuality compared to the total number of friends is considered.
- centrality property of the trustee is calculated as follows[3]

$$K_{ij}^{MC}(t) = \frac{|M_{ij}|}{|N_i|} \quad \text{----- (6)}$$

where

$M_{ij}$  be the set of common friends between  $i$  and  $j$

$N_i$  is the set of trustee's friends.

## 7.6 Community of Interest (COI)

- The trustor and the trustee share common interest groups, is an indication of the degree of the common interest
- the trust level of the trustee based on COI is calculated as [3]

$$K_{ij}^{\text{Col}}(t) = \frac{|M_{ij}^{\text{Col}}|}{|N_i^{\text{Col}}|} \text{----- (7)}$$

- combine each TA through a linear equation with weighting factors as shown

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

# 8. MACHINE LEARNING BASED MODEL

## 8.1 Algorithm I: Clustering and Labeling [3]

---

### Algorithm I : Data Clustering and Labelling

---

```
1:   Input:  $\underline{X}$    Output:  $\underline{y}$ 
2:   Initialize cluster centroids  $\mu_1, \mu_2, \dots, \mu_k \in \mathbb{R}^n$ 
3:   for  $k=1$  to 5 do
4:     Repeat until convergence: {
5:       for  $i=1$  to  $m$  do
6:          $c^{(i)} := \arg \min_j | | \mathbf{X}^{(i)} - \mu_k | |^2$ 
7:          $\mu_k :=$  Average of points assigned to cluster
8:        $k$ 
9:     end for
10:    }
11:     $J^{(k)}(c, \mu) := \arg \min_k J(c, \mu)$ 
12:  end for
13:  Optimum  $k \leftarrow$  Elbow method  $\leftarrow$  plot  $J^{(k)}$  vs  $k$ 
14:  for  $i=1$  to  $m$  do
15:    if  $c^{(i)}$  close to  $(0,0)$ 
16:       $y^{(i)} = 0$ 
17:    elseif
18:       $y^{(i)} = 1$ 
19:    end if
```

---

## 8.1.1 Principal Component Analysis [3]

---

Algorithm : Principal Component Analysis

---

- 1: Compute dot product matrix:  $\Sigma = X^T X$
  - 2: Compute eigenvectors:  $[U, S, V] = \text{SVD}(X^T X)$
  - 3: Specify the required dimension  $d$ :  $U_d = [u_1, \dots, u_d]$
  - 4: Compute  $d(=2)$  features:  $Z = U_d^T X$
-

## 8.2 Algorithm II: Classification Model[3]

---

### 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  $\gamma$ 
4:  for  $c, \gamma=0.01$  (multiple of 3) 30 do
5:    model=svmtrain( $\underline{y}, \underline{X}, \text{RBFK}, c, \gamma$ )
6:    prediction=svmpredict( $\underline{y}_{val}, \underline{X}_{val}, \text{model}$ )
7:    error [ $c, \gamma$ ] = predictions  $\neq y_{val}$ 
8:  end for
9:  Choose  $c, \gamma \leftarrow \text{minimum [error]}$ 
10:  [ $\text{weights}, \text{accuracy}, \text{decision values}$ ]
11:                                     = svmtrain( $\underline{y}, \underline{X}, \text{RBFK}, c, \gamma$ )
```


---

## 9. Conclusion

- Trust prediction model, which can correctly identify the trust boundaries of any interactions
- learn the best parameters to combine each TA to obtain a final trust value, is proposed based on the well-known SVM model.
- Algorithm is proposed to check whether an incoming interaction is trustworthy, based on several trust features corresponding to an IoT environment.
- Provides ability and accuracy of algorithm with respect to identifying trustworthiness interaction.

# 10. 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 930-93
- [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 6<sup>th</sup> 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.





**Thank You..**