International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2021 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Trust Management for Device to Device Communication in Internet of Thing using Learning Techniques

Rajkumar V. Patil, Parikshit N. Mahalle and Gitanjali R. Shinde

Department of Computer Engineering, Shrimati Kashibai Navale College of Engineering, Savitribai Phule Pune University, Pune

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

IoT has emanate out of advance in communication and information Technologies. IoT can be used in vast applications that can be used to simplify the needs of human beings. The IoT can be implemented in fields like Smart cities, homes, healthcare etc. In IoT device communicates with other devices many issues and challenges comes in picture regarding security and privacy. Trust management and how to calculate the trust score is one of the important issue. In this paper issues regarding calculations of trust score and trust management is proposed. The proposed method in this paper makes trust score calculation promising. The Fuzzy based method is proposed in this paper. The fuzzy approach used in paper uses three linguistic values for six parameters which are calculated from data collected from IoT devices. In this paper, we have also generated real-time datasets. We generate two datasets and compare them to check our approach of calculating the trust score is correct or not. Then this datasets are given to a proposed machine learning model. This proposed model can be used to predict trust score in IoT application.

Keywords: *Fuzzy Approach, Internet of things (IoT), Trust Score, Device to Device communication, Trust Management*

Introduction

The IoT has emerged out in field of information and communication technology has taken a series of changes in human life. Over the past several years, the development of communication and the internet make all the things into reality. Internet of Things means the wireless network of devices which are used in application like office and home automation, Smart City etc. The device used in this application is with selfconfigure capability [2]. In IoT, there are different types of computing devices in millions and billions of a number, they have different size and they can communicate with each other. The Decentralized nature of the IoT environment faces the challenges in security, Trust Management, Privacy and Identity Management (IDM) [3]. IoT devices should be highly secure, they should private, effective IDM and Trust Management. Trust gives the device a decision making power to make a judgment on other devices similar to how humans make the decision about other humans based on how much that person trust on the other. If a person trust high to other then he get much access and the other person can be secure to that person or viceversa. A Trust relationship between two devices can decide the upcoming interaction between those two devices. When two devices trust each other they love to share information, Resources to a certain level according to the trust level. This issue can be addressed by fuzzy-based trust calculation and trust management for device to device communication using machine learning. This paper uses a fuzzy approach to calculate the trust. This paper uses calculated value of Experience (Ex) [1-3], Knowledge (Kn) [1-3], Recommendation (Rc) [1-3], Honesty (Ho) [4], Cooperativeness (Co) [4] and Responsibility (Re) [4]. Real-time Dataset is generated by collecting the data from the IoT Devices then calculating Ex, Ho, Kn, Rc, Co, and Re. After calculating all the parameter we have used a fuzzy approach to calculate the trust value and its crisp value by the defuzzification method. In this paper we have generated two data at different time on same IoT devices. These two Dataset generated is then compared. Then this data set is given to proposed machine learning model.

This paper is organized as follow. Section II presents related work. Section III presents Gap Analysis. Section IV presents all the calculations related to calculating the trust. Section V present the generation of datasets. Section VI present proposed machine leaning model. Section VII finally concludes the research and discuss future work.

Related Works

Many Research are done on Trust Management for IoT devices. Many different formulas for calculating trust score has proposed by different researchers. Many of them view trust as a binary that is trusted or untrusted.

In 1996 M. Blaze et al. [5] has first introduced the concept of trust management, Authors have implemented a prototype 'Policy Maker Interpreter, which has the AWKWARD interpreter and built-in a regular expression. Indrajit Ray and Sudip Chakraborty in [6] define the trust and evaluate the trust relation between A -> B communication Authors have defined and evaluate three-parameters that are Knowledge, Recommendation and Experience which helped in evaluating the trust. Authors come up with computed trust by trust vector defined in [6]. An FTBAC (Fuzzy approach to the trust-based Access Control) Framework is proposed by P. N. Mahalle et al. [7]. Authors used the mamdani type fuzzy rule-based model. Three linguistics values that is Experience, Knowledge and Recommendation are used by the Authors in the Mamdani rule based model. The output of the model was fuzzy set {Good, Average, Low}. An FTBAC Framework includes three layer Device layer, Request Layer and Access Control Layer. According to trust value access is given to devices. . Fenye Bao et al. in [8] proposed a protocol which uses three-parameters from the human behavior (Honesty, Cooperativeness and Community Interest) to evaluate the trust. Trust value is a real number which ranges between 0 to 1 where 0 indicates distrust, 0.5 ignorance and 1 as a complete trust. Siri Gulenge et al. in [9] proposed a multi-agent trust management scheme for decentralized VNET. Authors have used fuzzy logic based approach to calculate the trust. Authors have used threeparameter Cooperativeness factor, Honestness Factor and Responsibility factor to calculate the trust. Authors have calculated and evaluated the Cooperativeness factor, Honestness Factor and Responsibility factor with the single connecting device that is A - > B. Author feed this parameter to fuzzy model. Sudip Chakraborty et al. in [10] come up with TrustBAC that is Trust based access control. Authors have extended Role based access control system to Trust based access control system. In [10] trust level determine by three factors – the past behavior that is experience, the knowledge and other device recommended the device that is recommendation. TrustBAC can choose one or all this factors to determine the trust level. In [1] machine learning approach is used to compute the trust for IoT services. Authors first evaluated the trust parameters and feed them to unsupervised machine learning model to label the data and then SVM is used to predict the new interaction as trust or distrust. All the above trust management models for the distributed and decentralized systems are sufficient for today's world. As IoT is growing day by day three parameters used in a fuzzy approach [7] and [9] will be not more useful for the growing world. This paper proposed a fuzzy approach for trust management using six parameters which is used to calculate the trust. Also, this paper practically generates datasets using the fuzzy approach. Then this dataset is feed to machine learning model discus in section VI.

Gap Analysis All the methods and models proposed [1-10] are designed according to today's system. As IoT grows day by day
huge amount of data is collected. To calculate the trust after every interaction can cause loss in energy and performance. From [5-7] three parameters used to calculate the trust score are sufficient for present IoT systems but for the modern world, we need more parameters to calculate trust score. For consuming energy and increase performance some artificial system is needed to calculate the trust score efficiently.

Trust Calculation

The proposed trust score calculation is divided into two part in this paper. The First part is for calculating the parameter used for calculating the trust score. The Second part is to calculate trust score using the fuzzy approach. This Section are presented below.

A. Calculating Ex, Ho, Kn, Rc, Co, Re

Before evaluating the parameters we like to define two characteristics of trust. The dynamic nature of trust that trust changes over a time and propensity to trust [1]. In this section 1 transaction = n number of interaction in particular time period between two device.

A.1 Calculating Experience (Ex) Experience (Ex) of trustor about a trustee is defines as a number of interactions between the trustor and a trustee in a particular time period.

Assuming that there is total n_i interaction in j^{th} interval of time. E_k^j is the value of the experience of k^{th} interaction. In case of successful interaction E_k^j value will be equals to +1 and in case of failure interaction E_k^j value will be equals to -1.

Experience for j^{th} interaction is given by Ij

$$I = \begin{cases} 0, & \text{if } n E = 0 \\ \dfrac{\sum}{\sum}, & \text{if } n E \neq 0 \end{cases}$$

I_j is the experience for every interaction for a particular time period.

So, Experience Ex for A on B in context c is given by

$$Ex = \frac{\sum w I}{\sum i}$$

Where n is the number of past Experience form past n transaction.

For Experience be in a range [-1, 1] we multiply weight w_i for i^{th} number of transaction and it is given by

( ) w = _ ∀i = 1,2, … … n And S = _____

A.2 Calculating Honestness (Ho) High Honestness (Ho) says that node or device is honest and send packet honestly to another device. Honestness is calculated as

$$Ho(m) = \begin{cases} \frac{N_S(m)}{N_T}, & \text{if } N < N \text{ and } N \neq 0 \\ 1, & \text{Otherwise} \end{cases}$$

Where $N_S(m)$ is the number of the successful packets forwarded by m and N_T is the total number of packets sent by m. Ho(m) is Honestness for a particular time interval.
$Ho_i(m) \leftarrow (1-\beta) \times Ho_{(i-1)}(m) + \beta \times Ho_i(m)$ Where $Ho_i(m)$ is present value of Honestness and $Ho_{(i-1)}(m)$ is past value of Honestness and β is weight associated with it β Є [0,1]. Honestness ranges between 0 to 1.

A.3 Calculating Knowledge (Kn)
Knowledge (Kn) given by

$$K = W_S + W_F$$

Where S,F is in range [-1,1], W_S , W_F in range [0,1] and $W_S + W_F = 1$, S and F are the number of successful interaction and failure interaction. W_S and W_F are the weight corresponding to S and F. Knowledge Kn Є [-1, 1]

A.4 Calculating Recommendation (Rc)
Recommendation (Rc) is given by

$$Rc = \frac{\sum R_{A \longrightarrow B} . I}{\sum R_{A \longrightarrow B}}$$

Where $R_{A \longrightarrow B}$ is successful interactions divided by the total interactions in a particular time period. Recommendation (Rc) is also in the range between [-1,1]

A.5 Calculating Cooperativeness (Co)
Cooperativeness (Co) given by

$$Co(A \rightarrow B) = \begin{cases} \frac{N_T(A \rightarrow B)}{N}, & \text{if } N(A \rightarrow B) < N \\ 1, & \text{otherwise} \end{cases}$$

Where N_T (A→B) is total package forwarded for a particular time interval say i and N_a is average of past n successful forward packets. Co(A) is cooperativeness for a
particular time interval now Co(A→B)i will be cooperativeness of A on B

$$Co(A \rightarrow B) = (1 - \beta)Co(A \rightarrow B) + \beta Co(A \rightarrow B)$$

$Co(A \rightarrow B)_{i-1}$ is past value Co(A→B)i and Co(A→B)i is present value of the cooperativeness of A on B and β is weight associated with it β Є [0,1] Cooperativeness (Co) ranges between
[0, 1]

A.6 Calculating Responsibility (Re)
Responsibility (Re) given by

$$Re(m) = \begin{cases} \frac{N_{R(m)}}{N_a}, & \text{if } N < N \text{ and } N \neq 0 \\ 1, & \text{Otherwise} \end{cases}$$

Where $N_{R(m)}$ is the total successful interactions for a particular time period with the neighbor and N_a is the average of past n successful transactions. Re(m) is responsibility for a
particular time interval. $Re_{i(m)}$ will be responsibility of device m

$$Re_i(m) \leftarrow (1- \beta) \times Re_{(i-1)}(m) + \beta \times Re_i(m)$$

$Re_{i-1(m)}$ is past value $Re_{i(m)}$ and $Re_{i(m)}$ is present value of Responsibility of A on B and β is weight associated with it β Є
[0,1]. Responsibility (Re) ranges between [0, 1]

B. Calculating Trust

To calculate the trust we used the Fuzzy approach. We used the Mamdani-type [11] [12] fuzzy rule based model which uses linguistic values Ex, Ho, Kn, Rc, Co, Re. The output of the model is the fuzzy set and the output value is converted to crisp value by the defuzzification method at the center of gravity (COG) [13].

$$COG(A) = \frac{\int \mu(x)x\,dx}{\int \mu(x)\,dx} \qquad COG(A) = \frac{\sum \mu(x)x}{\sum \mu(x)}$$

Trust can be said as a function of Ex, Ho, Kn, Rc, Co, Re

T = f(Ex, Ho, Kn, Rc, Co, Re)
Output of this function is fuzzy set given by
T = {Trust, Ignorance, Distrust}

This fuzzy set value is converted to crisp value by defuzzification method mention above.

Table 1 show linguistic value Experience, Recommendation and Knowledge and Table 2 show the linguistic value of Cooperativeness and Responsibility. Table 3 show the linguistic value of Honesty

Table 1: linguistic value of experience, recommendation and knowledge

L(Ex)	L(Rc)	L(Kn)	Fuzzy numbers
Bad	Negative	Insufficient	[-1,-1,0.1,0.25]
Average	Neutral	Less	[0.2,0.3,0.5,0.6]
Good	High	Complete	[0.5,0.7,0.8,1]

Table 2: linguistic value of cooperativeness and responsibility

L(Co)	L(Re)	Fuzzy Numbers
Less	Bad	[0, 0, 0.45]
Average	Average	[0,0.45,0.9]
Good	Good	[0.45,0.9,1,1]

Table 3: Linguistic Value Of Honesty

L(Ho)	Fuzzy Number
Dishonest	[0, 0, 0.8]
Partial	[0,0.8,1]
Honest	[0.8,1,1]

Figure 1, 2, 3, 4, 5, 6 shows the membership function Experience, Honesty, Knowledge, Recommendation, Cooperativeness and Responsibility respectively.

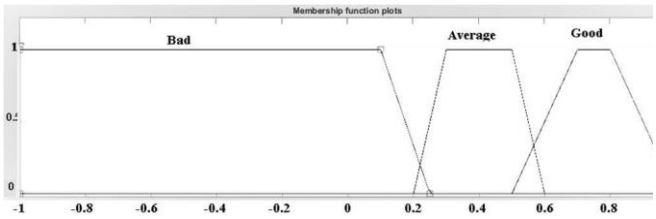

Figure 1: Membership function for experience

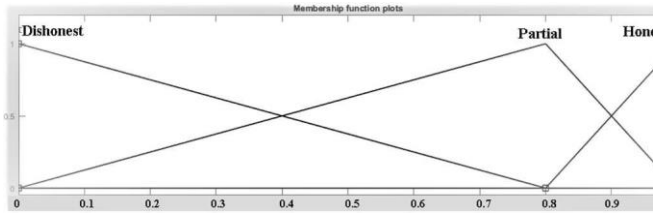

Figure 2: Membership function for Honesty

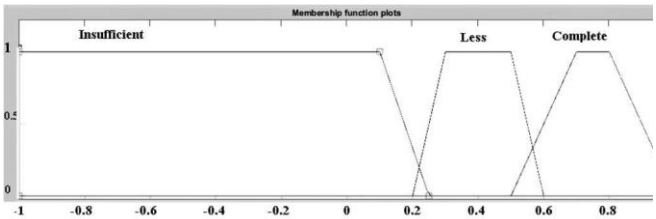

Figure 3: Membership function for Knowledge

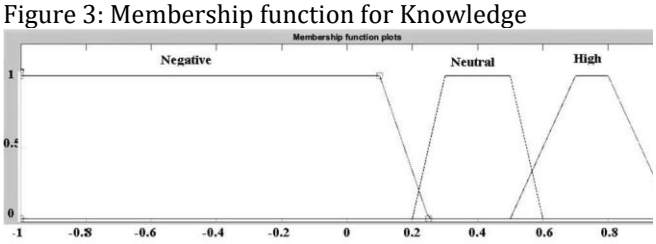

Figure 4: Membership function for Recommendation

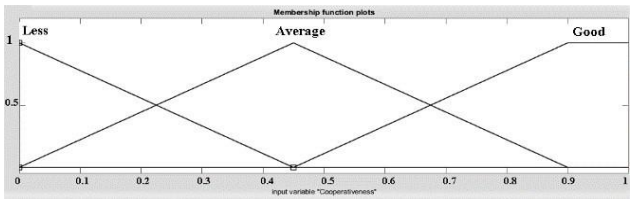

Figure 5: Membership function for cooperativeness

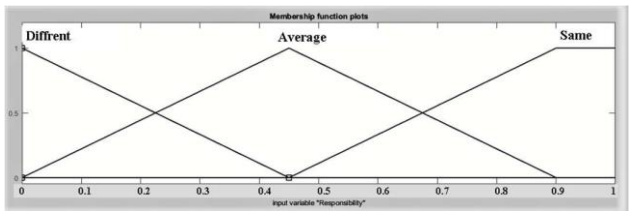

Figure 6: Membership function for Responsibility

Table 4 shows the linguistic value for the output variable trust and Figure 7 shows the Membership function for the output Trust.

Table 4: Linguistic Value Of Trust

L(T)	Crisp Range	Fuzzy Value
Distrust	Below 0.6	[0,0,0.6]
Ignorance	0.6 to 0.9	[0.6,0.8,0.9]
Trust	Above 0.9	[0.85,1,1]

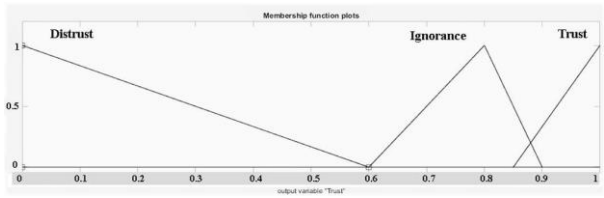

Figure 7: Membership function for output (TRUST)

Step 2 is to develop a fuzzy rule as there are six parameters and all have three linguistic value (Good, Average and Bad) so 3^6 = 729 rules can be made we taken all the rules in consideration out of that few are shown in Table 5

Table 5: Fuzzy Rule Set (Few of them)

Rule	If Ex	And Ho	And Kn	And Rc	And Co	And Re	Then T
1	Bad	Dishonest	Insufficient	High	Good	Good	Trust
2	Bad	Dishonest	Insufficient	High	Good	Average	Ignorance
3	Bad	Dishonest	Complete	Negative	Less	Average	Ignorance
4	Bad	Dishonest	Complete	Negative	Less	Bad	Distrust
5	Bad	Dishonest	Complete	Negative	Good	Good	Trust
6	Average	Dishonest	Insufficient	High	Average	Average	Ignorance
7	Average	Dishonest	Insufficient	High	Average	Bad	Distrust
8	Average	Dishonest	Insufficient	High	Good	Good	Trust
9	Good	Honest	Less	Neutral	Average	Bad	Ignorance
10	Good	Honest	Less	Neutral	Good	Good	Trust
11	Good	Dishonest	Less	Negative	Less	Bad	Distrust
12	Good	Dishonest	Less	Negative	Average	Good	Ignorance

Step 3 is to calculate the fuzzy value output by putting values of Ex, Ho, Kn,. Rc, Co and Re to interface/Libraries. The Output will be fuzzy set {Distrust, Ignorance, Trust}. Step 4 is to calculate the crisp value from fuzzy set and that is done by central of

gravity defuzzification method as discussed above. The range of Trust value is between [0, 1]

In the next section, we are going to see how to generate the dataset and calculate the trust. We have also compared the two datasets generated at different times.

To generate a dataset we have calculated Experience, Honesty, Knowledge, Recommendation, Cooperativeness and Responsibility by Equations discussed in section IV. We have also calculated trust as discussed in Section IV. We used 7 nodes A, B, C, D, E, F and G and they are connected to each other by 3 switch and 1 router. Switch 2, Switch 3 and router is connected to Switch 1 by the wired medium. Node A is connected to Switch 2 by the wired medium. Node B, C, D, E is connected to Switch 3 by the wired medium and Node F and Node G is connected to the router wirelessly. Using Python libraries we have connected all the nodes. Then we continuously forwarded ICMP packages of 400bytes, 600bytes and 800bytes to any of the node for 60 sec while generating dataset 1 and 30sec while generating dataset 2. After sending continuous packages we have capture sender node, receiver node, time period of forwarding packages, total packages forwarded, total successful packages forwarded and package loss. Also, we have find maximum, average and minimum time to send single ICMP package. Also, we have used TCP and UDP connection to forward the packages. The next step was to calculate the all six parameters form data generated as discussed above. We have calculate it by equation used in Section IV. The next step is to calculate trust using the fuzzy approach as discussed in section IV (Calculate Trust). We have calculated both fuzzy and the crisp value for trust. Dataset 1 has total of 1931 rows and Dataset 2 has total of 4499 rows. In Section V.I we will compare dataset 1 vs dataset 2Figure 8 shows the Datasets some rows. Hader row contains Client, Server, Experience, Honesty, Knowledge, Recommendation,

Cooperativeness, Responsibility, Crisp output and Trust value. 4 Steps to generate dataset

Step 1. Design a network and start communication between them (Section V).

Step 2. Extract sender node, receiver nod, total packages send, dataset it was observed that as communication increases the trust total successful packages send and package loss between devices increases but by very less number. Step 3. Calculate Ex, Ho, Kn, Rc, co, Re(Section IV.A)

Step 4. Calculate Trust (Section IV.B) and generate dataset.

Client	Server	Experience	Honesty	Knowledge	Recommendation	Cooperativeness	Responsibility	Crisp_Output	Trust_Value
A	B	0.1667	1.0000	1.0000	1.0000	1.0000	1.0000	0.9000	Trust
A	B	0.3600	1.0000	0.9999	1.0000	1.0000	1.0000	0.9000	Trust
A	B	0.5277	1.0000	1.0000	1.0000	0.5258	0.5258	0.9000	Trust
A	B	0.5277	1.0000	1.0000	1.0000	0.2840	0.2840	0.7929	Ignorance
A	B	0.5233	0.9868	0.8973	0.9827	0.6420	0.6420	0.9063	Trust
A	B	0.5125	0.9919	0.9877	0.9806	0.8210	0.8210	0.9045	Trust
A	B	0.3506	0.4963	0.9972	0.9701	0.4930	0.4106	0.5726	Distrust
A	B	-0.0283	0.7480	0.9992	0.9960	0.3345	0.2933	0.4496	Distrust
A	B	0.1829	0.8392	0.7411	0.9320	0.6673	0.6466	0.8164	Ignorance
A	B	0.3226	0.4205	0.9930	0.9310	0.4366	0.3235	0.4986	Distrust
A	B	-0.2038	0.2486	0.7167	0.7278	0.3279	0.1702	0.3625	Distrust
A	B	-0.3178	0.6243	1.0000	0.8654	0.6639	0.5851	0.7929	Ignorance
A	B	0.2078	0.7759	0.7311	0.8622	0.8320	0.7925	0.8405	Ignorance
A	B	0.4874	0.8880	1.0000	0.9541	0.4492	0.4295	0.7929	Ignorance
A	B	0.3534	0.4938	0.6413	0.8452	0.3467	0.2269	0.5887	Distrust
A	B	0.0255	0.7405	0.9497	0.9020	0.6734	0.6135	0.8123	Ignorance
A	B	0.2204	0.8702	0.9995	0.9019	0.4321	0.4021	0.4999	Distrust
A	B	0.5233	0.9350	0.9995	0.9914	0.3073	0.2923	0.8001	Ignorance
A	B	0.3613	0.4688	0.9900	0.9973	0.6537	0.1491	0.8007	Ignorance

Chart 1 show a comparison between Dataset 1 and Dataset 2. Chart 1 clearly shows that there is not too much different between Distrust, Ignorance and Trust value which means our method of calculating the trust is correct. Table 6 shows the compression.

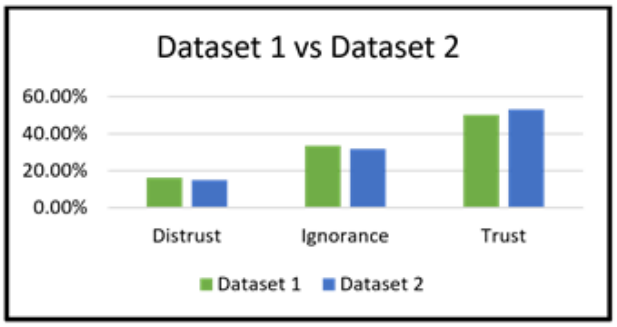

Chart 1: Dataset 1 vs Dataset 2

TABLE 7: DATASET 1vs DATASET 2

	DATASET 1	DATASET 2
DISTRUST	16.3	15.05
IGNORANCE	33.6	31.8
TRUST	50.2	53.1

By comparing this two dataset i.e. Dataset 1and Dataset 2 we can say that our calculation is correct. Also by comparing two datasets it is observed that only 50-55% fully trusted

This is how we can calculate the trust and prevent sending the important package to the untrusted devices. The datasets generated above and equation which are mention in

VI. PROPOSED MACHINE LEARNING MODEL

Figure 9 shows the machine leaning model. We have randomly generated 3 data frame from dataset that we have generated in section V. Each data frame is given to three different algorithm i.e. Random Forest (RF), Naive Bayes (NB) and Decision Tree (DT). By voting classification final model get generated. Test data is feed to model and accuracy of Model is calculated of system. Proposed Model is divided in 3 level: Level 1 split the dataset in 3 train Dataset Randomly, Level 2 is train data is send each algorithm describe in figure 9 and generate the 9 model, Level 3 takes output of each model and perform maximum voting classification.

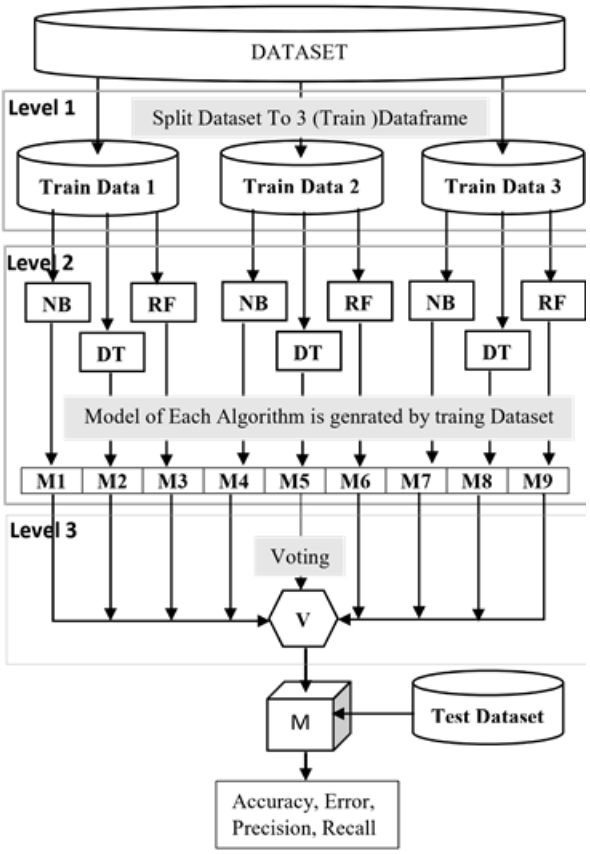

Figure 9 Proposed Machine Learning Model

communication and 15-20% Untrusted communication. In a

In this Paper we have taken whole Dataset 1(Discuss in section V) as train dataset and split it into 3 train dataset randomly and Dataset 2(Discuss in section V) is taken as a test dataset. Splitting of dataset is done using sklearn library and Gaussian distribution is used to create the category of data because Naive Bayes need categorical dataset as an input. Those Train Datasets are passed to Naïve Bayes, Decision Tree and Random Forest algorithm and model is created as shown in figure 9. Again sklearn libraries of python are used create a models of these algorithm (NB, DT, RF). Size of train data set is [(1931, 9)] and test dataset [(4499,)]. Total 9 models are trained according to proposed system model in figure 9 M1, M2 to M9. Then next in next level voting is done. The maximum class will win the voting election and the class will be the final predicted output of model or proposed system. Output is in set of [Distrust (Class 0), Ignorance (Class 1), and Trust (Class 2)]. After the model/proposed model is trained. The Test dataset i.e dataset 2 is passed to proposed model and performance of model is measured shown in table 8. Table 8 shows the different between NB vs DT vs RF vs
Proposed Model on basis of accuracy and error rate

TABLE 8: RANDOM FOREST (RF) VS NAIVE BAYES (NB) VS DECISION TREE VS PROPOSED MODEL
Model Naive Bayes Decision Tree Random Forest Proposed model
Performance %
Accuracy 87.014 94.377 95.532 96.177
Error 12.986 5.623 4.468 3.823

Table 8 shows that proposed model has highest accuracy then other 3 model (Random Forest (RF), Naive Bayes (NB) and Decision Tree (DT)). Table 9 shows the Confusion Matrix and table 10 shows Precision, Recall, f1-score, Support of all three class and there average and total value.

TABLE 8: RANDOM FOREST (RF) VS NAIVE BAYES (NB) VS DECISION TREE VS PROPOSED MODEL

Model / Performance %	Naive Bayes	Decision Tree	Random Forest	Proposed model
Accuracy	87.014	94.377	95.532	96.177
Error	12.986	5.623	4.468	3.823

TABLE: 9 CONFUSION MATRIX

Predicted / Actual	Class 0 (Distrust)	Class 1 (Ignorance)	Class 2 (Trust)	Total
Class 0	646	31	0	677
Class 1	37	1384	11	1432
Class 2	0	93	2297	2390
Total	683	1508	2308	4499

TABLE 10: PRECISION, RECALL, F1-SCORE, SUPPORT

Class	Precision	Recall	F1-score	Support
0(Distrust)	0.95	0.95	0.95	677
1(Ignorance)	0.92	0.97	0.94	1432
2(Trust)	1.00	0.96	0.98	2390
Avg/Total	0.96	0.96	0.96	4499

In this paper the proposed model describe above in this section is the most accurate then Random Forest (RF), Naive Bayes (NB) and Decision Tree (DT).

Conclusion And Future Work

In Internet of things for D2D commination there are many challenges and issues related to security, privacy, access control, identity management etc. One important issue and challenge is the trust management. In this paper, we have proposed a method to calculate the trust using the fuzzy approach. A Fuzzy model uses six parameters as an input and returns a fuzzy set of Trust as the output. This paper also proposed the method to generate real time dataset using fuzzy based model. We have generated 2 datasets and compare both dataset. A machine learning model is proposed in this paper which can be used in future work.

In future work, we like to apply machine learning on datasets to make the artificial system. This fuzzy approach can also be used in an access control mechanism. Trust calculation can be used in IoT applications like smart city, Home and Office automation, meteorology department etc.

References

[1]. U. Jayasinghe, G. M. Lee, T. W. Um, Q. Shi, "Machine Learning based Trust Computational Model for IoT Services", IEEE Transactions on Sustainable Computing (Volume: 4 , Issue: 1 , Jan.-March 1 2019)

[2]. M. Weiser, “The computer for the 21st century,” In Scientific American, Volume: 265, pp: 66-75, September 1991.

[3]. M.M. Ollivier, "RFID: a new solution technology for security problems", European Convention on Security and Detection, pp. 234-238, May 1995.

[4]. Ing-Ray Chen, Fenye Bao, Jia Guo, "Trust-Based Service Management for Social Internet of Things Systems", IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 6, pp. 684-696, November/December 2016. [5]. M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized Trust Management” In Proceedings of the IEEE Symposium on Research in Security and Privacy, pp: 164, Oakland-CA, May 1996.

[6]. Indrajit Ray and Sudip Chakraborty “A Vector Model of Trust for Developing Trustworthy Systems” In Proceedings of the 9th European Symposium of Research in Computer Security (ESORICS 2004), volume 3193 of Lecture Notes in Computer Science, pages 260–275, Sophia Antipolis, France, September 2004.

[7]. P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, “A Fuzzy Approach to Trust Based Access Control in Internet of Things,” In Proceeding of the 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE). IEEE, June 2013, pp. 1–5.

[8]. F. Bao, nd I. R. Chen, "Trust Management for the Internet of Things and Its Application to Service Composition," IEEE WoWMoM 2012 Workshop on the
Internet ofThings: Smart Objects and Services, San Francisco, CA, USA, 2012

[9]. S. Guleng, C. Wu, X. Chen, X. Wang, T. Yoshinaga, and Y. Ji, “Decentralized trust evaluation in vehicular Internet of Things,” IEEE Access, vol. 7, pp. 15980_15988, 2019.

[10]. Sudip Chakraborty, Indrajit Ray “TrustBAC-Integrating Trust Relationships into the RBAC Model for Access Control in Open Systems” //Symposium on Access Control Models and Technologies- SACMAT’06. Lake Tahoe: IEEE Computer Society, 2006: 49-58.

[11]. Timothy J. Ross, “Fuzzy Logic with Engineering Applications,” Third Edition © 2010 John Wiley & Sons, Ltd, ISBN: 978-0- 470-74376-8. [12]. T.J. Procyk and E.H. Mamdani, “A linguistic self-organizing process controller,” In Automatica, Volume: 15, pp: 15-30, 1979.

[13]. L. A. Zadeh, “Fuzzy sets,” In Information and Control Journal, Volume: 8, Issue: 3, pp: 338-353, June 1965.