International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Access Control through Trust Management in Ubiquitous Computing under Uncertain Environment

D. S. Shelar[1*], P. B. Shinde[2], Santosh D. Jadhav[3], P. A. Thakre[4], N. S. Mujumdar[5]

Submitted: 16/02/2024 **Revised**: 13/03/2024 **Accepted**: 21/03/2024

Abstract*:* This paper describe the trust calculation method in ubiquitous computing under uncertain environment where the access is granted on having successful interactions with other devices/agents. Many researchers including us proposed the trust models where the quality features like recommendations, history, authenticity, credibility, transitivity, mobility and reliability of requester agents have been considered. But if above quality features are vague in nature, the existing model does not seem to be suitable. With this inspiration we proposed fuzzy logic based model in which the uncertainty occurred due to vagueness in various parameters like credibility, transitivity and reliability can be captured so as to get the better results and compared the results with the results obtained in [11]. This trust calculation model can be incorporated in Ubiquitous Computing for better decision making with respect to the access control when uncertainties are involved in quality features.

Keywords: *Fuzzy Logic, Access Control, Ubiquitous Computing, Trust, Credibility Mobility, Reliability, Transitivity.*

1. Introduction:

In the 2021 century, Computer technology plays a very important role in human daily life because it integrates the public and privet sectors like industry, logistics, transportation, and the medical field through electronic devices. In order to address those issues, Mark Weiser [1] introduced the paradigm shift from one to one computer to one to many computers with the help of ubiquitous computing (Ubicomp) in which electronic nodes are fully connected and make them available for sharing and processing the data because Ubicomp has capacity to remove the complexities of computing so that the various activities can be done efficiently with optimal use of memory.

Ubicomp provides access to all electronic user nodes on the basis of smart interactions. The smart interaction refers to the interaction made with the credible nodes which provide trustworthy information. If a user is trustworthy, the experience will be worthy even if the product is not perfect in a business transaction. If node Q is trusted by node P, they are going to stay loyal to every alternative. As a result, loyal nodes are extraordinarily helpful during access control management strategy to grant access to other electronic nodes/agents. The main task of ubiquitous computing is to maintain privacy which may cause its popularity to decrease.

The emergence of these devices has created many security issues for which existing mechanisms are not sufficient, especially concerning the problems of authentication and user’s private data protection. So, one of the important threats of ubiquitous computing is to maintain privacy which may cause its popularity to decrease. Many researchers contributed a lot to data security in access control for Ubicomp. Hua Wang [2] and his team presented an access control model to protect services and devices in the Ubicomp environment, which allows the access restrictions directly on services and object documents. This model provides a mechanism to build relationships between models and objects. Finally, comparisons with related works are analyzed.

In this study, we proposed a Fuzzy Logic model for the calculation of trust by capturing uncertainties that occurred in input parameters like credibility, reliability and transitivity keeping mobility of an agent in access control as a crisp quantity for Ubicomp and also tried to present the best solution for access control in an uncertain environment.

The remaining section of the paper is organized as follows: In Section 2 the preliminaries of fuzzy sets are presented. Section 3 explains the motivation for our model. Sections 4 describe the literature review of the various approaches regarding trust models in Ubicomp. The proposed fuzzy logic model for trust calculation is presented in Section 5

1. Department of Engineering Sciences, AISSMS Institute of Information Technology, Pune, India

2. Department of Engineering Sciences, AISSMS Institute of Information Technology, Pune, India

3. Department of General Engineering, N. K. Orchid College of Engineering &Technology, Solapur, India

4. Department of Engineering Sciences, Zeal College of Engineering and Research. Pune, India

5. Department of Engineering Sciences, JSPM’s Rajarshi Shahu College of Engineering Pune, India

** Corresponding Author Email: dilipsshelar@gmail.com*

followed by application and trust calculation in Section 6. Finally experimental results and conclusion are presented in Section 7 and Section 8 respectively.

2. Preliminaries:

2.1 Fuzzy Sets:

Classical set theory says that every element 'x' must be either in the set or not. It is useful for the characterization of objects for which complete precision is possible like either the thing is yes or no, true or false, one or zero and cold or hot. The characteristic functions of classical set theory map elements of some universal set X into the binary {0,1}. So it is defined as:

$$\chi_A(x) = \begin{cases} 1 \text{ for } x \in A \\ 0 \text{ for } x \notin A \end{cases}$$

However, such exactness is not always possible. If there are 100 men with different age groups, we can't say that these many men are old, young or middle age. Such ambiguity frequently pervades human thinking, and it is reflected in human language. In order to deal with such ambiguity and imprecision Lotfi A. Zadeh (1965) invented fuzzy set theory and presented a precise mathematical tool for processing data that is derived from vague information. In fuzzy set theory the characteristic function from the binary set {0,1} is extended to the interval [0, 1], where the characteristic function is labelled as membership function (μ) which takes the values of universal set to the interval [0, 1].

Definition 1:

Fuzzy set: Fuzzy set is a function defined on some universal set X and its range is the interval [0, 1] that is $\mu_A: X \to [0,1]$. Hence, a fuzzy set consists of a set of objects with their membership values.

Definition 2: $\boldsymbol{\alpha}-$cut : $\alpha-$cut of fuzzy set is a crisp set such that the membership values of it are $\geq \alpha$

$$A^\alpha = \{x \in X \mid A(x) \geq \alpha\} \quad where\ \alpha \in [0,1]$$

Note: In above definition if $\geq$ is replaced by > then it is called strong $\alpha - cut$ of fuzzy set A.

Theorem 1: Two fuzzy sets are equal if and only if all their corresponding α-cuts are equal.

$$A^\alpha = B^\alpha <=> A = B\,, \qquad \forall\alpha$$

Definition 3: The height of a fuzzy set A is the maximum membership value gained by A(X) over universal set X

$$h(A) = \sup(x)\,, x \in X$$

Definition 4:

Fuzzy Number: Let R be the set of real numbers. A fuzzy set defined on domain R is called a fuzzy number if fuzzy set is normal $\{x \,/\, A(x) = 1 \text{ for atleast one } x\}$and it has bounded support if $\{x/A(x) > 0\}$.

Definition 5:

Trapezoidal Fuzzy Numbers (TRFN): It is a fuzzy set described by following membership function.

$$T_r(x) = \begin{cases} \dfrac{x-a}{l-a} & , \text{ for } a \leq x \leq l \\ 1 & , \text{ for } l \leq x \leq r \\ \dfrac{x-b}{r-b} & , \text{ for r} \leq x \leq b \end{cases}$$

$$Where\ a \leq l \leq r \leq b$$

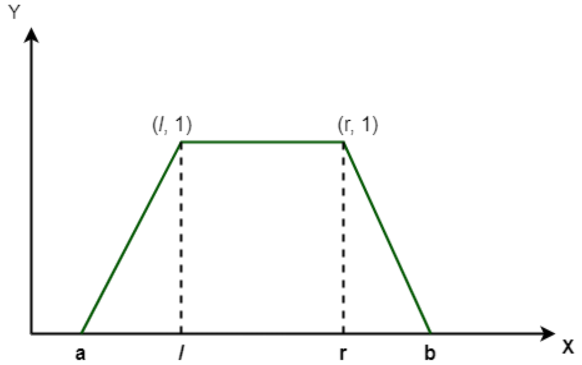


Fig.1: Membership function of trapezoidal fuzzy Number.

2.2: Fuzzy Logic

The Logic governed by fuzzy set is called Fuzzy Logic (FL). FL theory allows us to work on reality linguistically using linguistic variables. Linguistic variables are an entity which takes values is fuzzy sets. FL represents a new approach to the system modelling. E. H. Mamdani reported the first known application of Zadeh's theory where inputs are compared to membership functions by a process called fuzzification in which the membership function is assigned to each linguistic term. The logic combinations of linguistic terms are then evaluated by application of FL operators: usually minimum grade of membership is selected as a fitness grade of the fuzzy rule in the following multi-input single-output form as under.

R1 IF (x_1 is X_{11}) **and ………and** (x_n is X_{1n}) THEN (y is Y_1)

R2 IF (x_1 is X_{21}) **and ………and** (x_n is X_{2n}) THEN (y is Y_2)

.

.

RN IF ($x_1$is X_{N1}) **and ………and** (x_n is X_{Nn}) THEN (y is Y_N)

Here $x \in X$ with the membership value $\mu_X(x)$.

For the sake of simplicity R1 can be written as

$$\text{If } x_1 \text{ } is \text{ } X_1 \textbf{and} \ldots . \textbf{and} \text{ } x_n \text{ } is \text{ } X_n \text{ then } y \text{ } is \text{ } (a_0 + a_1 x_{1+\ldots} a_n x_n),$$

where $a_1 \ldots a_n$ are constants.

For particular imputes, Let $\mathrm{x}_1 = \mathrm{x}_1{}^0$, $\mathrm{x}_2 = \mathrm{x}_2{}^0, \ldots \ldots \mathrm{x}_\mathrm{n} = \mathrm{x}_\mathrm{n}{}^0$ belong to $\mathrm{X}_1, \mathrm{X}_2 \ldots \mathrm{X}_\mathrm{n}$ respectively with membership values $\mu_{X_1}(\mathrm{x}_1{}^0) \ldots \ldots \ldots \mu_{X_n}(\mathrm{x}_\mathrm{n}{}^0)$, the output variable is

$$\mathrm{y}^0 = a_0 + a_1 \mathrm{x}_1{}^0 + \cdots + a_n \mathrm{x}_\mathrm{n}{}^0$$

Therefore the membership value of $y = y^0$ is

$$\mu_Y(\mathrm{y}^0) = \sup\{(\mu_{X_1}(\mathrm{x}_1{}^0)\wedge \ldots \ldots \ldots \wedge \mu_{X_n}(\mathrm{x}_\mathrm{n}{}^0)\}$$

And the corresponding membership values for all outputs is

$$\mu_Y(y_i^0) = \sup_{y_i^o = a_{io} + \ldots . + a_{in} x_n^o.} \{(\mu_{X_1}(\mathrm{x}_1{}^0)\wedge \ldots \ldots \ldots \wedge \mu_{X_n}(\mathrm{x}_\mathrm{n}{}^0)\}$$

where $i = 1,2 \ldots \ldots n$.

By center of gravity defuzzification method the value of output variable y is

$$y = \frac{\sum_{i=1}^{i=N} \mu_Y(y_i^0) . y_i^0}{\sum_{i=1}^{i=N} \mu_Y(y_i^0)}$$

In this study, we have built the fuzzy rules by considering linguistic terms of quality features. This model is based on if-then rules of Mamdani fuzzy inference system in which we can control the process so as to get the desired trust value.

The General structure of a fuzzy logic controller in Fuzzy Inference Engine (FIS) is shown in following figure.

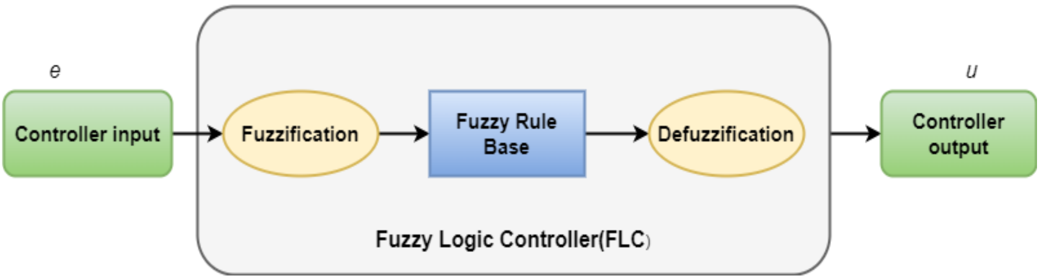


Fig.2: Fuzzy Inference Engine

3. Motivation:

In today’s world, technology, including social media, has strongly influenced a person’s life. Anyone can freely share information based on relationships only through communication and even by developing new relationships with people with who are not familiar. This type of relationship may cause the disclosure of the privacy of a person. So, it is very important to verify the trustworthiness of the people/user-agent when we are sharing valuable information with them. There must be a mechanism to access the access control policy regulated by the owner/user.

For Electronic Social media [24-26] there are a lot of traditional access control mechanisms are available today to solve the problem but due to the dynamic owner-user relationship, it has its limitations. Private information is not secured after a certain period because the owner may disclose the information. Therefore it is very essential to keep vigil on the user behavior continuously and also necessary to check the trustworthiness of users. To address this issue Baek and Kim [23] introduced the dynamic trust-based access control for the online social network

In their work they can decide whether the access should be granted to the user or not by evaluating the trust values also can monitor negative behavior.

Ubiquitous computing concerning access control using trust is an emerging field in network security. The existing literature mentioned that trust is an alternative to collaborating in a world without passwords and necessary certificates. It seems to be the logical choice that we are simply to integrate its workings and mechanisms into our new security concepts for ubiquitous computing. Although trust-based access control is picking up speed in the field of ubiquitous computing by giving access to electronic users to compute the ‘trustworthiness ‘of other electronic users depending on their interactions. But it is not clear when it comes to defining the problem we are trying to solve. So naturally, the question arises what is the role of trust in the access control in Unicomp?. Such type of queries can be addressed by giving access to the agent by the positive interactions happening with even third-party users. In the literature, most of the work available is related to ubicomp and focused on expanding the concept of trust from a network security point.

Not only does grant or denying access of depending on pre-computed certificates but also it depends on a particular context. We have been motivated to present the fuzzy logic-based model because of uncertainty in parameters like credibility, reliability and transitivity keeping mobility as a crisp parameter.

4. Literature Review:

Mark Weiser [1] articulated the idea of ubiquitous computing for the first time at the Computer Science Lab at Xerox Palo Alto Research center (PARC). One of the important things in the ubicomp is the trust between the agents for rendering the access to other agents and it’s naturally helping to deal with the security issue.

Decentralized trust-management Policymaker proposed by M. Blaze et.al [9] in that they have shown the comprehensive approach to trust management which is depend on simple language for trusted actions and trust relationships that will facilitate the development of security features in a wide range of network services.

Jameel et al. [10] invented the trust model which is based on the vectors of trust values of different entities in ubicomp by capturing uncertainties that occurred in his model. Colin English [12] proposed that trust and cryptographic security are considered to be orthogonal to each other by assuming the existence of reliable encryption techniques and focusing on the characteristics of a model that supports the management of the trust relationships between two devices during ad-hoc interactions.

R. He et al. [13] and his team presented a trust management framework for a multi-cloud environment to evaluate the trustworthiness of Cloud Service Providers and Trust Service Providers based on trust management architecture using subjective and objective trust. Trust management model to manage the trust and its properties for ‘software as a service in a cloud computing environment presented by Prajapati et al.[15].

Malika Yaici et al.[16] suggested a context-aware authentication system using trust management between client and servers and also proposed Trust calculation.

Shelar et al. [11] presented the experimental results using the best suited mathematical model for access control through trust management in ubiquitous computing to provide access to the requester-agent/node. Also shown that the presented trust calculation leads to better decision making with respect to weightage of three attributes like credibility, transitivity and reliability.

Fuzzy approach to the Trust-Based Access Control model is proposed by Mahale et al. [7]. They also presented where the trust is calculated using uncertain parameters. An Experience model for Ubicomp was proposed by Nalini Mhetre et al.[8]. They suggested a new mathematical model for the experience of nodes with other nodes by considering the parameters such as history, reliability, and transitivity, and ubiquity to grant access control.

5. Proposed Model:

Existing fuzzy trust based access control model (FTBACM) [7] calculate trustworthiness of each device or group of devices based

on three uncertain components such as knowledge, experience and recommendation but the proposed trustworthiness model presented in this article with attributes like Credibility(C_r), Reliability (R_l), Transitivity T(z) and Mobility(M_b) of requester agent where C_r, R_l and T(z) are considered as the linguistic variables and M_b belongs to [0, 1] as crisp variable.

5.1. Credibility

Recently wide range of impacts is created by Electronic Social media in our day-to-day life. But the owners are facing the challenges of being susceptible to wrong information and rumours. In order to deal with this issue, the credibility of user nodes in social media needs to be checked. Jiaxi Sun [22] proposed new formula to evaluate the credibility of social media information which is based on user perception. The credibility of news propagated is presented by Castillo et al. [20].Barbier and Liu [21] introduced a method to find provenance paths leading to sources of the information to evaluate its credibility. So, we have considered one of the quality features of access control that is creditability of user nodes with the help of interactions happened between user nodes and owner nodes.

Let F_k be the previous interaction happened between the agent where values of $F_k \in [0\,,1]$, $k = 1,2, \ldots.,n$.

Then the credibility $(C_r) = \frac{\sum_{k=1}^{i=n} F_k}{n}$; $0 \le C_r \le 1$

Since the credibility value is context dependent, owner has to decide which credibility value gets fitted to his/her model. Shelar et al.[11] has taken the value of credibility equal to 0.8 for the agent to be considered as credible. But it may be unjustifiable if $C_r = 0.8$ is credible and 0.79 is not credible. In order to justify it we have considered C_r as a linguistic variable and tried to contribute in obtaining suitable trust value of an agent-node by taking linguistic terms as Highly Credible(HC), Credible(C), Moderately Credible(MC) and Low Credible(LC).

Category and linguistics term	Range	Trapezoidal Fuzzy numbers
Highly Credible(HC)	$C_r \geq 0.9$	$(0.8, 0.9, 1, 1)$
Credible(C)	$0.8 \leq C_r < 0.9$	$(0.7, 0.8, 0.9, 1)$
Moderately Credible(MC)	$0.7 \leq C_r < 0.8$	$(0.6, 0.7, 0.8, 0.9)$
Low Credible(LC)	$C_r < 0.7$	$(1, 1, 0.7, 0.8)$

- Membership Function of Highly Credible (HC) is

$$\mu_{HC}(x) = \begin{cases} 1 & ; \quad x \geq 0.9 \\ \dfrac{(x-0.8)}{1} & ; \ 0.8 \leq x < 0.9 \\ 0 & ; \quad x < 0.8 \end{cases}$$

- Membership Function of Credible (C) is

$$\mu_C(x) = \begin{cases} \dfrac{(x-0.7)}{1} & ; \quad 0.7 \leq x < 0.8 \\ 1 & ; \quad 0.8 \leq x < 0.9 \\ \dfrac{(1-x)}{0.1} & ; \quad 0.9 \leq x < 1 \end{cases}$$

- Membership Function of Moderately Credible (MC) is

$$\mu_{MC}(x) = \begin{cases} \dfrac{(x-0.6)}{0.1} & ; \quad 0.6 < x \leq 0.7 \\ 1 & ; \quad 0.7 < x < 0.8 \\ \dfrac{(0.9-x)}{0.1} & ; \quad 0.8 \leq x < 0.9 \end{cases}$$

- Membership Function of Low Credible (LC) is

$$\mu_{LC}(x) = \begin{cases} 1 & ; \quad x < 0.7 \\ \dfrac{(0.8-x)}{0.1} & ; \quad 0.7 \leq x < 0.8 \\ 0 & ; \quad \mathrm{x} \geq 0.8 \end{cases}$$

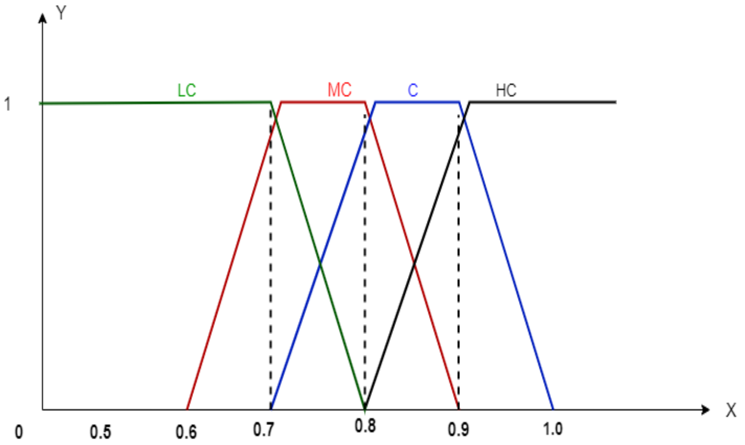


Fig. 3: Membership function for Credibility

5.2: Transitivity

Interaction between the two agents happens smoothly if their experience was good. But in a trust management system, an agent P is not directly interacted with an agent R due to absence of authentication between them. Here the trust transfer plays an important role through intermediate agent Q. Trust transfer happens only if an agent Q recommends to an agent P that an agent R is trustworthy if an agent P is a trustor and agent Q is a trustee. It may happen that magnitude of trust will be different amongst agents Q and R and P and R.

Recently the big task in access control is to figure out the trust between the unknown agents these issues can only solve through trust transitivity. There are several research articles available on this issue. Josang et.al [17] described trust transitivity in online interaction among strangers using belief operators. Xiang Quiteet. al. [18] presented a trust transitivity model based on a theory of evidence by capturing uncertainty occurring in the model. Xu and Fung [19] introduced a risk-defined trust transitivity model for group decision-making in social networks. They used risk-defined trust propagation operator which propagate trust and distrust information, based on risk-bearing defining factors like trust, distrust, uncertainty, and inconsistency.

Shelar et al.[11] calculated transitive trust by minimizing trusts between two pairs of trust values. If the magnitudes of trust between agents P, Q, and Q, R are known then the trust between P and R can be calculated as follows.

Let x, y and z be the trust between (P, Q), (Q, R) and (P, R).

$$\mathrm{z} = \min(x, y) = \mathrm{T(z)}, \quad \text{where } x, y, z \in [0,1].$$

But the question may arise; if trust value ‘z’ is not crisp then the trust transitivity may not perform one of the important contributors in overall trust calculation between two agents. This issue may be addressed by taking ‘z’ as trapezoidal fuzzy number T(z) with linguistic terms Very Good (VG), Good (G), Average(AVG) and Low.

Category of Trust Transitivity	**Range**	**Trapezoidal Fuzzy numbers**
Very Good(VG)	$T(z) \geq 0.8$	$(0.7, 0.8, 1, 1)$
Good(G)	$0.7 < T(z) < 0.8$	$(0.6, 0.7, 0.8, 0.9)$
Average(AVG)	$0.6 < T(z) < 0.7$	$(0.5, 0.6, 0.7, 0.8)$
Low	$T(z) < 0.6$	$(1, 1, 0.6, 0.7)$

- Membership Function of Very good Transitivity (VG) is

$$\mu_{VG}(z) = \begin{cases} 1 & ; \quad z \geq 0.8 \\ \dfrac{(z-0.7)}{0.1} & ; \ 0.7 \leq z < 0.8 \\ 0 & ; \quad z < 0.7 \end{cases}$$

- Membership Function of Good Transitivity (G) is

$$\mu_{G}(z) = \begin{cases} \dfrac{(0.9-z)}{0.1} & ; \quad 0.8 \leq z \leq 0.9 \\ 1 & ; \quad 0.7 \leq z < 0.8 \\ \dfrac{(z-0.6)}{0.1} & ; \quad 0.6 \leq z < 0.7 \end{cases}$$

- Membership Function of Average Transitivity (AVG) is

$$\mu_{AVG}(z) = \begin{cases} \dfrac{(z-0.5)}{0.1} & ; \quad 0.5 \leq z \leq 0.6 \\ 1 & ; \quad 0.6 < z < 0.7 \\ \dfrac{(0.8-z)}{0.1} & ; \quad 0.7 \leq z \leq 0.8 \end{cases}$$

- Membership Function of Low Transitivity (Low) is

$$\mu_{Low}(z) = \begin{cases} 1 & ; \quad z \leq 0.6 \\ \dfrac{(0.7-z)}{0.1} & ; \quad 0.6 \leq z < 0.7 \\ 0 & ; \quad \mathrm{z} \geq 0.7 \end{cases}$$

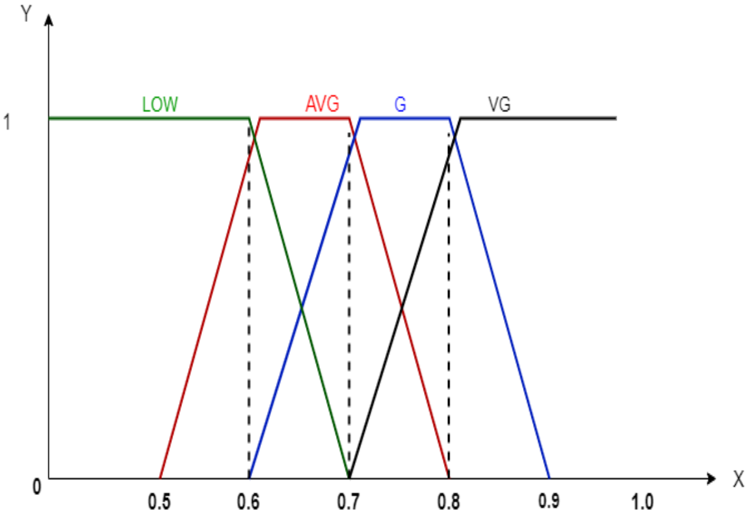


Fig. 4: Membership function for Transitivity

5.3: Reliability

The accuracy of the reliability value is important to measure trust. In the Ubicomp environment, access is granted only when the particular agent is reliable. Reliability can be calculated when the agent shows consistently excellent performance in the past interaction. When Node P is reliable to node Q only if P consistently keeps good interactions with Q. It may be invited less reliability when the interaction happened in a short period or very less consistent interaction happened.

In a wire-less sensor network (WSN) only a highly reliable agent will get access. There are many interactions happened between the two agents in two different time span in months or years during the business. An agent is said to be reliable [11] when the two sets of interactions are correlated up to the desired level. Shelar et al.[11] addressed this issue by figuring out the coefficient of correlation between two sets of interaction-values.

Let $(f_k)_{t_1}$and $(f_k)_{t_2}$ be the interaction values between two agents in time slot t_1 and t_2 respectively.

The correlation coefficient between $(f_k)_{t_1}$and $(f_k)_{t_2}$:

$$r_l = \frac{\sum_{\mathrm{j=1}}^{j=n}\{[(f_k)_{t_1} - (f_l)_{t_1}]\ [(\mathrm{f}_k)_{t_2} - \overline{(\mathrm{f}_l)}_{t_2}]\}}{\sqrt{[(\mathrm{f}_k)_{t_1} - \overline{(\mathrm{f}_l)}_{t_1}]^2[(\mathrm{f}_k)_{t_2} - \overline{(\mathrm{f}_l)}_{t_2}]^2}}$$

Where (i) $\overline{(f_l)}_{t_1}$and $\overline{(f_l)}_{t_2}$be the mean values of$(f_k)_{t_1}$ and $(f_k)_{t_2}$ respectively.

(ii) $-1 \leq r_l \leq 1$

For convenience the reliability factor, we considered $R_k = |r_l|$

In this study, we have considered R_k as a linguistic variable with linguistic terms such as highly reliable(HR), reliable(R), moderately reliable(MR) and less reliable (LR).

Category and linguistics term	Range	Trapezoidal Fuzzy numbers
Highly Reliable (HR)	$R_k \geq 0.9$	$(0.8, 0.9, 1\ , 1)$
Reliable (R)	$0.8 \leq R_k < 0.9$	$(0.7, 0.8, 0.9, 1)$
Moderately Reliable (MR)	$0.7 \leq R_k < 0.8$	$(0.6, 0.7, 0.8, 0.9)$
Low Reliable (LR)	$R_k < 0.7$	$(1, 1, 0.7, 0.8)$

- Membership Function of Highly Reliable (HC) is

$$\mu_{HR}(x) = \begin{cases} 1 & ; \quad x \geq 0.9 \\ \dfrac{(x-0.8)}{1} & ;\ 0.8 \leq x < 0.9 \\ 0 & ; \quad x < 0.8 \end{cases}$$

- Membership Function of Moderately Reliable (MC) is

$$\mu_{MR}(x) = \begin{cases} \dfrac{(x-0.6)}{0.1} & ; \quad 0.6 < x \leq 0.7 \\ 1 & ; \quad 0.7 < x < 0.8 \\ \dfrac{(0.9-x)}{0.1} & ; \quad 0.8 \leq x < 0.9 \end{cases}$$

- Membership Function of Reliable (C) is

$$\mu_R(x) = \begin{cases} \dfrac{(x-0.7)}{1} & ; \quad 0.7 \leq x < 0.8 \\ 1 & ; \quad 0.8 \leq x < 0.9 \\ \dfrac{(1.0-x)}{0.1} & ; \quad 0.9 \leq x < 1.0 \end{cases}$$

- Membership Function of Low Reliable (LC) is

$$\mu_{LR}(x) = \begin{cases} 1 & ; \quad x < 0.7 \\ \dfrac{(0.8-x)}{0.1} & ; \quad 0.7 \leq x < 0.8 \\ 0 & ; \quad \mathrm{x} \geq 0.8 \end{cases}$$

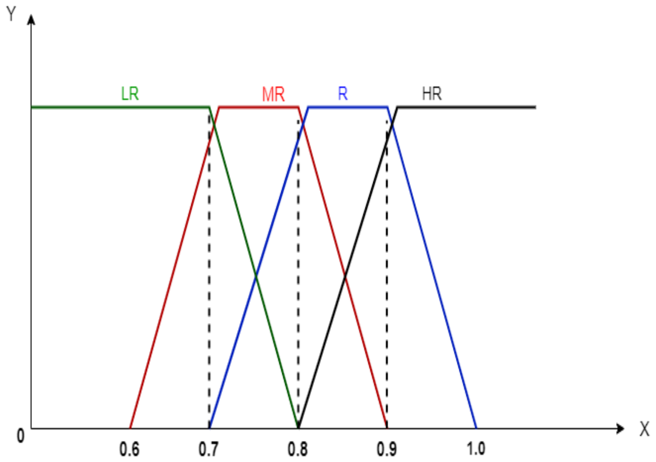


Fig. 5: Membership function for Reliability

5.4: Mobility

Mobility is the main reason for changes in the circumstances of any interaction that happened between the agents. There are several variations of mobility that are considered such as Adhoc mobility, device mobility, code mobility, session mobility, etc. Mobility is one of the important aspects when a large number of agents play in Ubicomp**.** In online social networks (OSN) to build up relationships, users provide access to unknown requester-agents even if it is mobile (not stationary). If the requester-agents move far away from the user-agent, in this case, the proper interaction may not happen this may result in the risk of disseminating unclear information.

So, in order to address this issue Shelar et al.[11] used the mobility factor-range of requester-agents which is one of the important contributors to trust calculations. Access is granted to the agent when the distance of the requester-node from the user-node is within the specific range.

Let $\delta_1$and δ_2 be the positions of requester-agent and user-agent respectively.

Let s be the distance between $\delta_1$and δ_2 that is $d(\delta_1, \delta_2) = s$ and $R_{(\delta_1, \delta_2)}$be the region covered by user-agent.

$$R_{(\delta_1, \delta_2)} = \{x/d(\delta_1, \delta_2) \leq s\}$$

If a requester-agent lies in the region $R_{(\delta_1, \delta_2)}$ then the interaction may happen whether it is successful or nor it is immaterial. In this case we assign the value of mobility factor is 1 else 0. In our study we kept mobility factor as a crisp quantity. If the mobility factor is in the specified range the requester-agent is entitled for other quality features otherwise trust will not be calculated for that particular requester-agent means access will be denied. In this study we kept mobility factor as it is as mentioned in [11].

6. Application and Trust Calculation:

In this FL model following steps are used

1. Selection of fuzzy input and fuzzy output as a trapezoidal fuzzy numbers.
2. Formation of fuzzy rules base using Mamdani model.
3. Getting output as a crisp value of trust.

Trust Calculation:

Since access control and the trust are closely related and the value of trust is calculated on the basis of C_r, R_l, T(z) and $M_b$with their linguistic terms, this paper proposes to use the trust as a tool in decision making of access control in Ubicomp under uncertain environment where the linguistic terms for fuzzy trust values are taken to be Low Trust (LT), Moderate Trust (MT), Trust (T) and High Trust (HT).Trust value (T_r) as an output can be obtained by developing rule base under Mamdani inference engine. There may be all possible 264 rules. But for the sake of simplicity we have taken 12 rules.

Membership functions of all linguistic terms are as follows.

- Membership Function of Low Trust (LT) is

$$\mu_{LT}(x) = \begin{cases} 1 & ; \quad x \leq 0.6 \\ \dfrac{(x - 0.6)}{0.1} & ; \; 0.6 < x < 0.7 \\ 0 & ; \quad x \geq 0.7 \end{cases}$$

- Membership Function of Moderate Trust (MT) is

$$\mu_{MT}(x) = \begin{cases} \dfrac{(x - 0.5)}{1} & ; \quad 0.5 \leq x < 0.6 \\ 1 & ; \quad 0.6 \leq x < 0.7 \\ \dfrac{(0.8 - x)}{0.1} & ; \quad 0.7 \leq x < 0.8 \end{cases}$$

- Membership Function of Trust (T) is

$$\mu_{T}(x) = \begin{cases} \dfrac{(x - 0.6)}{0.1} & ; \quad 0.6 < x \leq 0.7 \\ 1 & ; \quad 0.7 < x < 0.8 \\ \dfrac{(0.9 - x)}{0.1} & ; \quad 0.8 \leq x < 0.9 \end{cases}$$

- Membership Function of High Trust (HT) is

$$\mu_{HT}(x) = \begin{cases} 0 & ; \quad x \leq 0.7 \\ \dfrac{(x - 0.7)}{0.1} & ; \quad 0.7 \leq x < 0.8 \\ 1 & ; \quad \mathrm{x} \geq 0.8 \end{cases}$$

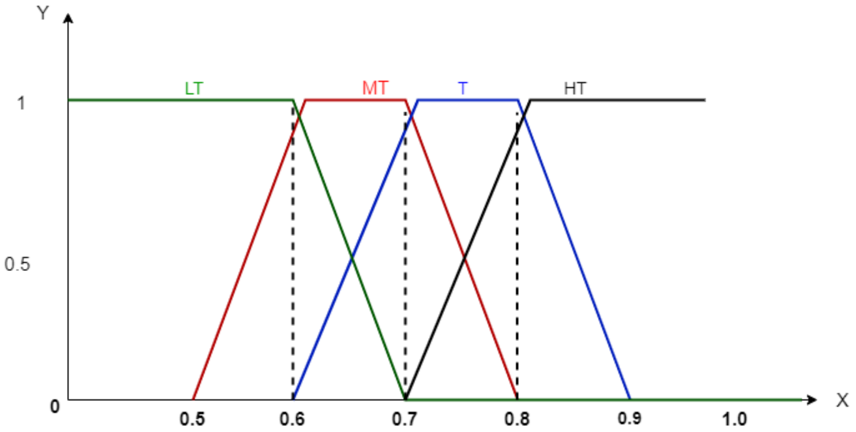
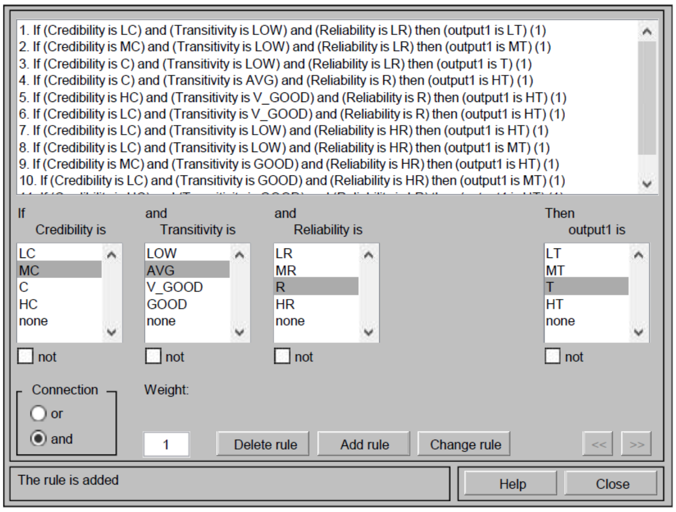


Fig: 6. Membership function of Trust


1. If (Credibility is LC) and (Transitivity is LOW) and (Reliability is LR) then (output1 is LT) (1)
2. If (Credibility is MC) and (Transitivity is LOW) and (Reliability is LR) then (output1 is MT) (1)
3. If (Credibility is C) and (Transitivity is LOW) and (Reliability is LR) then (output1 is T) (1)
4. If (Credibility is C) and (Transitivity is AVG) and (Reliability is R) then (output1 is HT) (1)
5. If (Credibility is HC) and (Transitivity is V_GOOD) and (Reliability is R) then (output1 is HT) (1)
6. If (Credibility is LC) and (Transitivity is V_GOOD) and (Reliability is R) then (output1 is HT) (1)
7. If (Credibility is LC) and (Transitivity is LOW) and (Reliability is HR) then (output1 is HT) (1)
8. If (Credibility is LC) and (Transitivity is LOW) and (Reliability is HR) then (output1 is MT) (1)
9. If (Credibility is MC) and (Transitivity is GOOD) and (Reliability is HR) then (output1 is HT) (1)
10. If (Credibility is LC) and (Transitivity is GOOD) and (Reliability is HR) then (output1 is MT) (1)

If Credibility is: MC
and Transitivity is: AVG
and Reliability is: R
Then output1 is: T
Connection: ● and
Weight: 1
The rule is added

Fig.7. Rule Base

7. Experimental results:

Shelar et al. [11] Performed an experiment on 15 requester-nodes in 9 scenarios and stated that 60%, 30% and 10% weightage should be given to the reliability, transitivity and credibility for obtaining trust value 0.8 or more. But in our study we have obtained the desired trust value even on having little less weightage in one of the three factors using Mamdani fuzzy rule-base inference engine.

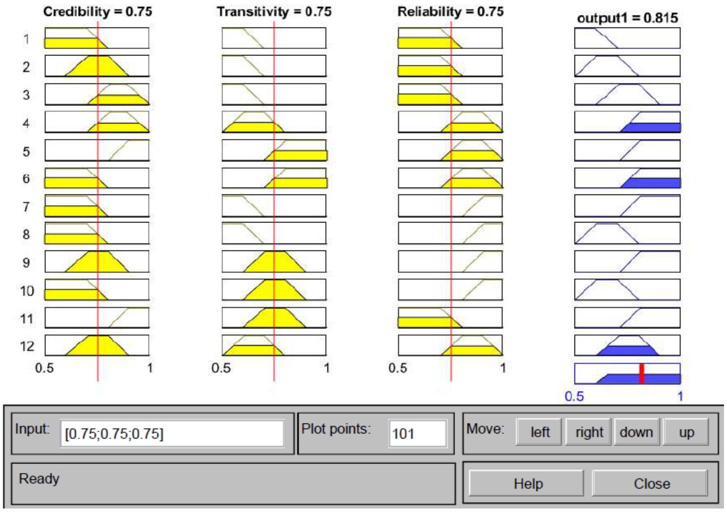

Credibility = 0.75
Transitivity = 0.75
Reliability = 0.75
output1 = 0.815
Input: [0.75;0.75;0.75]
Plot points: 101
Ready

Fig.8. Output as a Rule Viewer

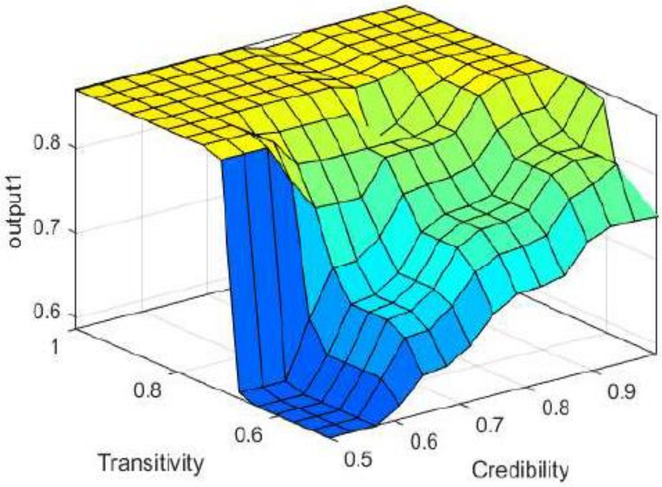


Fig.9. Output as Surface Viewer

8. Conclusion:

This paper presents the FL model for access control through trust management in ubicomp by mapping linguistic values of interaction-based parameters to the trustworthiness. Simulation results also shows that, even with the little less or more values of the parameters the desired trust value can be obtained, it may improve the decision making of owner-agent with respect to the grant or denial of access to the requester agent. This may also lead to the save the memory/energy of requester agents.

References

[1] Weiser, M. (1999). The computer for the 21 century. ACM SIGMOBILE Mobile Computing and Communications Review, 3(3), 1999, pp. 3–11. https://doi.org/10.1145/329124.329126

[2] Hua Wang, Yanchun Zhang, Jinli Cao, Access control management for ubiquitous computing, Future Generation Computer Systems 24, 2008, pp. 870–878. https://doi.org/10.1016/j.future.2007.07.011

[3] J. Seigneur, C. Jensen, Trust enhanced ubiquitous payment without too much privacy loss, ACM Symposium on Applied Computing, ACM Press, New York, NY, USA, 2004, pp. 1593–1599. https://doi.org/10.1145/967900.968218

[4] G. Sampemane, P. Naldurg, R. Campbell, Access control for active spaces, ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference, IEEE Computer Society, Washington, DC, USA, 2002, pp. 343-352. DOI:10.1109/CSAC.2002.1176306

[5] P. Viswanathan, B. Gill, and R. H. Campbell. Security architecture in gaia. Technical Report, University of Illinois at Urbana-Champaign, May 2001. http://gaia.cs.illinois.edu/papers/llncs.pdf

[6] J. Jai-muhtadi, R. Campbell, A. Kapadia, M. Mickunas, S. Yi, Routing through the mist: Privacy preserving communication in ubiquitous computing environments, Proceedings of the 22nd International Conference on Distributed Computing Systems, ICDCS'02, IEEE Computer Society, Washington, DC, USA, 2002,pp.74-83. https://homes.luddy.indiana.edu/kapadia/papers/mist.pdf.

[7] P. N. Mahalle, P. A. Thakre, N.R. Prasad, R. Prasad , A fuzzy approach to trust based access control in internet of things, 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems,VITAE,2013,pp.2–6. https://doi.org/10.1109/VITAE.2013.6617083.

[8] N. Mhetre, A. Deshpande, P. Mahalle, and P.Thakre, Experience Modelling For Ubiquitous Computing A Mathematical Approach, Turkish Journal of Computer and Mathematics Education,Vol.12,No.6(2021),pp.5476-5488. https://turcomat.org/index.php/turkbilmat/article/view/9735/7436

[9] M Blaze, J Feigenbaum, J Lacy, Decentralized trust management, 17th IEEE Symposium on Security and Privacy,Oakland,(1996),pp.164–173. .https://doi.org/10.1109/SECPRI.1996.502679.

[10] [H Jameel, LX Hung, U Kalim, A Sajjad, S Lee, Yk Lee, A trust model for ubiquitous systems based on vectors of trust values, 7th IEEE International Symposium on Multimedia, Irvine, USA, (Dec 2005),pp. 674–679. https://doi.org/10.1109/ISM.2005.22

[11] D. S. Shelar, P. G. Andhare, S. B. Gaikwad, P. A. Thakre, A Mathematical Model For Access Control Through Trust Management In Ubiquitous Computing, Stochastic Modeling & Applications,Vol.26,No.3(2022),1002-1009. https://doi.org/10.5281/zenodo.6572635.

[12] C English, P Nixon, S Terzis, A McGettrick, H Lowe, Security models for trusting network appliances, 5th IEEE International Workshop on Networked Appliances, Liverpool, (Oct2002),pp.39–44. http://dx.doi.org/10.1109/IWNA.2002.1241334

[13] R He, J Niu, M Yuan, J Hu, A novel cloud-based trust model for pervasive computing, 4th International Conference on Computer and Information Technology, China, (Sept 2004), pp. 693–700. http://dx.doi.org/10.1109/CIT.2004.1357276

[14] V Cahill, E Gray, J. Seigneur, C Jensen, Y Chen, B Shand, N Dimmock, A Twigg, J Bacon, W Wagealla, S Terzis, P Nixon, G Serugendo, C Bryce, M Carbone, K Krukow, M Nielsen, Using trust for secure collaboration in uncertain environments, IEEE Pervasive Computing Mobile and Ubiquitous Computing. 2(2003), pp. 52–61. DOI: 10.1109/MPRV.2003.1228527

[15] S. Prajapati, S.Changder, A. Sarkar, Trust Management Model for Cloud Computing Environment,Proceding of the International Conference on Computing. Communication and AdvancedNetwork-ICCCAN,2013,pp.509-513. https://doi.org/10.48550/arXiv.1304.5313

[16] Malika Yaici, A. Oussayah, M.Ahmed.Takerrabet, Trust Management for an Authentication System in Ubiquitous Computing, International Journal of Electronics and Communication Engineering Vol:12, No:6, (2018) pp.469-478. DOI:10.1016/j.procs.2018.07.141

[17] A. Jøsang Simon, Siman Pope, Semantic Constraints for Trust Transitivity, Conceptual Modelling, Second Asia-Pacific Conference on Conceptual Modelling(APCCM2005), Newcastle, NSW, Australia, 2005,pp.1-10. https://crpit.scem.westernsydney.edu.au/confpapers/CRPITV43Josang.pdf

[18] Xiang Qiu, Li Zhang, Shouxin Wang and GuanqunbQian, A Trust Transitivity Model Based-on Dempster-Shafer Theory, Journal of Networks, Vol. 5, No. 9, 2010, pp.25-32. https://doi.org/10.4304/jnw.5.9.1025-1032

[19] Jun Xu, Carol J. Fung, dblp Computer Science Bibliography. A Risk-defined Trust Transitivity Model for Group Decisions in Social Networks. IM 2019, pp. 415-420. https://dblp.org/rec/conf/im/XuF19.html

[20] . Castillo, M. Mendoza, and B. Poblete, Information credibility on twitter, In Proceedings of the 20th international conference on World wide web, ACM, 2011, pp. 675–684. https://doi.org/10.1145/1963405.1963500

[21] G. Barbier and H. Liu, Information provenance in social media. Social Computing, Behavioral-Cultural Modeling and Prediction, 2011, pp. 276–283. https://doi.org/10.1007/978-3-642-19656-0_39

[22] Jiaxi Sun, Research on the Credibility of Social Media Information Based on User Perception, Security and Communication Networks Volume 2021, pp.1-10. https://doi.org/10.1155/2021/5567610

[23] Seungsoo Baek, Seungjoo Kim, Trust-Based Access Control Model from Sociological Approach in Dynamic Online Social Network Environment, The Scientific World Journal, vol.1, 2014, pp.1-8. DOI: 10.1155/2014/936319

[24] [24] X. Qian, T. F. Lunt, A MAC policy framework for multilevel relational databases, IEEE Transactions on Knowledge and Data Engineering, vol. 8, no. 1, 1996, pp.3–15. .https://doi.org/10.1109/69.485625

[25] L. Snyder, Formal models of capability-based protection systems, IEEE Transactions on Computers, vol. 30, no. 3, 1981, pp. 172– 181. https://doi.org/10.1109/TC.1981.1675753

[26] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models", Computer, vol. 29, no. 2,1996, pp. 38–47. https://profsandhu.com/journals/computer/i94rbac(org).pdf

[27] L. A. Zadeh, Fuzzy set, Information and control, 8(1965), pp. 338-353. https://doi.org/10.1016/S0019-9958(65)90241-X .

[28]] L.A. Zadeh,Outline of A New Approach to the Analysis of complex Systems and Decision Processes, 1973.pp.28-44 DOI: 10.1109/TSMC.1973.5408575.

[29] L. A. Zadeh, Fuzzy algorithms Information and control, Vol 12 (1968), pp.94-102. https://doi.org/10.1016/S0019-9958(68)90211-8