A Trust Model for Ubiquitous Healthcare Environment on the Basis of Adaptable Fuzzy-Probabilistic Inference System

Georgia Athanasiou, George C. Anastassopoulos, Eleni Tiritidou, and Dimitrios Lymberopoulos, *Member, IEEE*

***Abstract*—Trust is considered to be a determinant on psychologist selection which can ensure patient satisfaction. Hence, trust concept is essential to be introduced into ubiquitous healthcare (UH) environment oriented on patients with anxiety disorders. This is accomplished by trust model estimating psychologists' trustworthiness, a priory to service delivery, with the use of patient's and his/her acquaintances testimonies, i.e., personal interaction experience and reputation (R). In this paper, a trust model is proposed to be materialized via an adaptable cloud inference system (ACIS) that performs trust value (TV) estimation. Taking advantage of a cloud theory, the introduced ACIS estimates TVs via fuzzy-probabilistic reasoning incorporating a cloud relation operator (soft AND) which is proposed to be tuned by trust information sources consistency and coherency. Theoretical analysis along with comparative study conducted within MATLAB environment and experimental investigation verify the effectiveness of the proposed ACIS materialization under different conditions. Especially, the innovative features of ACIS enable TV to be estimated with 45.5% and 62% on average higher accuracy to that providing state-of-the-art trust models, within clean environment and under the influence of large-scale collusive malicious attacks, respectively. The enhanced robustness permits the untrustworthy UH providers to be discriminated with true positive rate at the range of 0.9 although 40% of R testimonies are erroneous. Finally, experimental investigation validates that the adoption of the proposed trust model for psychologists trustworthiness estimation facilitates patient satisfaction to be achieved into UH environment.**

***Index Terms*—Cloud theory, reasoning, trust, ubiquitous healthcare.**

I. Introduction

WORLD Health Organization enlists anxiety disorders to epidemics of 21st century [1]–[4]. Anxiety disorders by impairing patients' task performing and decision making abilities, affect quality of everyday life [3], [5], [6]. The establishment of Ubiquitous Healthcare (*UH*) environment that enables personalized monitoring of patients' stress levels and psychological surveillance, without spatiotemporal limitations, is regarded as a promising alternative [7], [8].

Physiological signal analysis provides strong indicatives for stress event detection [9], [10]. However, contextual information contribute on stress detection and treatment to be ameliorated [11], [12]. For that purpose, mental healthcare domain argues about psychological questionnaires capturing hidden information on ambience. The problem is how to convince a patient who experienced a stress event to report his/her symptoms [6]. Hence, patient is important to believe on psychologist's technical proficiency and willingness to assist him/her [13], [14]. Essentially, mental healthcare domain regards trust as the necessary basis encouraging patient to reveal important medical information [15], [16]. From that perspective, psychologist selection in terms of trust significantly contributes on accomplishment of effective treatment and consequently determines patient's satisfaction [17], [18]. Considering lack of physical contact within *UH* environment, trust is essential to be introduced as key factor on *UH* Provider (i.e., psychologist) selection [13], [16], [19].

On the contrary, trust is already exploited on provider's selection in P2P, IoT and social networks [20]–[25]. Within that context, trust concept is materialized via Trust Models that foresight providers' trustworthiness in terms of Trust Values (*TV*s), a priori to service delivery [22]. Especially, *TV* estimation is based on trust information sources, i.e., Personal Interaction Experience (*PIE*) and Reputation (*R*) composed by service requestor's and other users' accumulated testimonies, respectively [23], [24]. In distributed environments, testimonies formulating *R* are derived by service requestor's acquaintances rather than all users interacted with a given provider [22]. Hence, accurate *TV* estimation from an observation sample (i.e., *PIE* and *R*) is a challenging issue in distributed Trust Models design [20]. In other words, modern research focuses on establishing a mathematical approach that deals with complexity and uncertainty of *TV* estimation in order accuracy to be achieved. *TV* estimation

Manuscript received February 4, 2017; revised June 18, 2017; accepted July 19, 2017. Date of publication July 27, 2017; date of current version June 29, 2018. *(Corresponding author: Georgia Athanasiou.)*

G. Athanasiou and D. Lymberopoulos are with the Wire Communication Laboratory, Electrical and Computer Engineering Department, University of Patras, Patras GR-26504, Greece (e-mail: gathana@ece.upatras.gr; dlympero@upatras.gr).

G. C. Anastassopoulos is with the Medical Informatics Laboratory, School of Medicine, Democritus University of Thrace, Alexandroupolis GR-68100, Greece (e-mail: anasta@med.duth.gr).

E. Tiritidou is with the Private Psychological Centre of Alexandroupolis, Alexandroupolis GR-68100, Greece (e-mail: tiritidou@gmail.com).

Digital Object Identifier 10.1109/JBHI.2017.2733038

accuracy is also essential to be preserved even in case that *R* includes erroneous testimonies generated by either autonomous or collusive malicious attacks. The key factor ensuring robustness against malicious attacks is trust information sources weighting. However, determination of weighting means and method still remains a hot topic since robustness against large scale and undercover collusive attacks is yet to be achieved.

Despite the abundant of literature, there is lack of Trust Model that serves the purpose of *UH* Provider's (i.e., psychologist's) selection. To cover the need for accurate *UH* Providers' trustworthiness estimation even in case of highly misleading malicious attacks, in this paper, Trust Model is proposed to be materialized by an Adaptable Cloud Inference System (*ACIS*). Taking advantage of cloud theory, *TV* is estimated via fuzzy-probabilistic reasoning that comprehensively deals with inherited uncertainty and hidden nonlinearities. In parallel, a cloud relation operator (*soft AND*) which is designed to be tuned by trust information sources consistency and coherency constitutes the basis of a novel weighting method. The ameliorated performance of the proposed Trust Model originates on both the innovative *ACIS* materialization and the utilization of coherency and consistency as weighing means expressing trust information sources dispersion range and deviation from normal modeling, respectively. Comparative study conducted within MATLAB simulation environment with the use of Epinions database verifies the proposed Trust Model enhanced accuracy and robustness over a wide range of malicious attacks including the undercover. In parallel, both simulation and experimental results indicate that the innovative ACIS implementation permits accurate discrimination between the trustworthy and the untrustworthy (*UH*) Providers not only in clean environment but also under the influence of large scale malicious attacks. Finally, the effectiveness for adopting the proposed Trust Model into a UH environment oriented on patients with anxiety disorders, is experimentally investigated in collaboration with Medicine School of Democritus University of Thrace.

The rest of the paper is organized as follows: The issues arising in Trust Models are presented in Section II. In Section III, cloud theory is described along with cloud-based representation of trust information sources. The proposed Trust Model is presented in Section IV. Trust Model implementation and evaluation are analyzed in Section V. In Section VI, experimental investigation about Trust Model effectiveness in psychologist's selection is presented. Finally, the paper concludes in Section VII.

II. Problem Statement

Literature reports a plethora of Trust Models designed for open and distributed environments. Trust Models deployed on weighted summation/average of trust information sources are referred as linear and categorized according to weighting method [15]. In similarity weighting is assumed that 1) similar users tend to have the same trust perspective, 2) partial knowledge included into *PIE* is closer to actual trustworthiness compared to R and 3) all users are truthful [24], [26]. In particular, similarity is computed not only by comparing *R* with *PI*E but also assessing contextual information [27]. The need for storing additional information makes similarity weighting resource consuming. As regards the second assumption which is mathematically expressed by complementary weighting of trust information sources (i.e., $(1-\alpha)PIE+\alpha R$) deprives accuracy from *TV* estimation since the fact that trust information sources are similar does not necessarily implies that reflect actual trustworthiness. Finally, the third assumption constitutes similarity-based Trust Models vulnerable to malicious attacks [24]. To cover this major disadvantage, machine learning algorithms, such as K-mean [19], and optimized weighting schemes [27], [23] are adopted. In that way, not only Trust Model complexity is increased but also performance depends on quality and stability of training dataset since training is required [18].

In linear Trust Models, credibility is also exploited as weighing mean. Credibility is approached as the difference between testimonies and global *TV*. However, this information is unlikely to be available in distributed environments [18]. Hence, Gaussian distribution is adopted for trust information sources representation where credibility is expressed via standard deviation [28]. However, distortion causing undercover attacks is unlike to be captured by credibility given that erroneous testimonies slightly deviate from the benevolent [19]. Similarly, the impact of collusive malicious attacks affecting less than 30% of *R* testimonies is not fully reflected on credibility variation [29]. To deal with robustness related issues, credibility is extended with the feature of abnormality on testimonies distribution quantified by percentiles or complex linearization methods [28], [29]. On that basis, false testimonies filtering schemes are developed. However, benevolent testimonies are highly possible to be outweighed, in case of complex malicious attacks and thus *TV* estimation process can be misled [19].

Trust Models deployed on probabilistic inference schemes, are also cited in literature. Particularly, Bayesian Network is utilized for similarity-based Trust Model materialization [14]. However, probabilistic inference is based on Beta or Gaussian distributions which require a wide range of testimonies in order to be precisely defined [20]. Hence, accuracy issues are raised in case of testimonies sparseness. Even though, the adoption of regression models permits accuracy issues to be faced, Trust Models complexity is increased [18], [26]. Additionally, the exploitation of similarity as weighting mean makes the given Trust Models highly vulnerable to malicious attacks. To meet this challenge, belief theory is combined with a probabilistic threshold scheme [22]. However, undercover malicious attacks affect probabilistic threshold stability. Additionally, the introduction of probabilistic threshold scheme into Trust Model increases complexity while scalability issues are raised [18]. In [24], a credibility-based Trust Model deployed on Expectation Maximization tunable Kalman filter, is described. However, the introduced optimal Gaussian estimator is affected by large scale malicious attacks, while undercover malicious attacks mislead probabilistic threshold scheme. On the contrary, the proposed, in this paper, Trust Model meets the challenges of accurate and robust TV estimation even in case of complex malicious attacks, as indicated in the following.

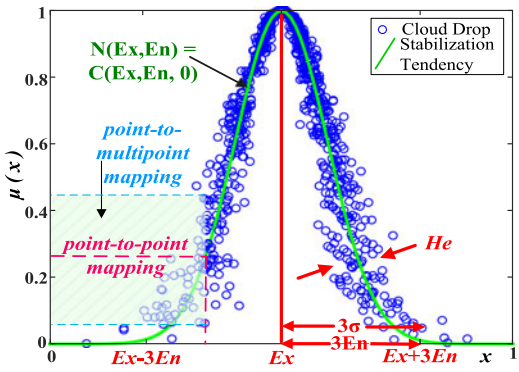

Fig. 1. Representation and analysis of Cloud C(0.5, 0.1, 0.03).

III. Approaching Trust Concept Via Cloud Theory

According to literature, Gaussian representation of trust information sources is more informative compared to single value [23], [24], [28]. That approach also enables stationary behavior to be removed from trust information sources representation [27]. However, the diversion of false testimonies from normal behavior introduces unpredictable errors into Gaussian representation which affect Trust Models accuracy [14]. To deal with this issue cloud theory is adopted for trust information sources representation [30].

A. Cloud Theory Basics

Beyond cloud computing paradigm, in literature is reported cloud theory as branch of Artificial Intelligence. Cloud theory is an improved qualitative-quantitative transformation model that captures correlated fuzziness and randomness of linguistic terms [31]. Let *C* be a qualitative concept related to a numerical set *U*. If there is a number $x \in U$ that randomly realizes C with certainty degree $\mu(x) \in [0, 1]$ which is a random value with stabilization tendency

$$\mu : U \rightarrow [0, 1] \; \forall x \in U \; x \rightarrow \mu(x) \tag{1}$$

then *x* distribution on *U* is defined as cloud and accordingly each *x* constitutes a cloud drop [32]. The approach of certainty degree as a random number highlights combination of fuzzy logic with probability theory [30].

Cloud is numerically defined by the triplet expectation value (*Ex*), entropy (*En*) and hyper-entropy (*He*), i.e., *C(Ex,En,He)* [33]. *Ex* is the mathematical expectation of cloud drops distribution in *U*. As shown in Fig. 1, the "*3En*" rule defines the region within a concept is acceptable to be represented [32]. *En* determines cloud drops dispersion in *U*. In contrast, *He* regulates cloud thickness which is the result of approaching certainty degree as distribution [31]. Essentially, *He* is the basis of point-to-multipoint mapping that cloud theory establishes for qualitative-quantitative transformation [33]. As indicated in Fig. 1, $He = 0$ declares that certainty degree is a fix number, i.e., point-to-point mapping of fuzzy logic. Therefore, *He* indicates cloud drops deviation from stabilization tendency which is modeled by $N(Ex, En^2)$. Finally, variance is defined as $\sigma^2 = En^2 + He^2$.

B. Cloud-Based Representation of Trust Information Sources

Trust Model exploits trust information sources formulated by dedicated mechanisms. Especially, after UH service delivery, a testimony is generated via Trust Assessment mechanism [15]. Mechanism takes as inputs service requestor's (i.e., patient) satisfaction from *UH* Provider (i.e., psychologist) stress management pattern and communication skills along with estimated stress level and *UH* service duration. The produced testimony, defined within the range [0,1], is introduced into Update mechanism that formulates *PIE* with the use of cloud algebra [30]. The emerged *PIE* is represented by $C_{PIE}(Ex_{PIE}, En_{PIE}, He_{PIE})$ where:

1) Ex_{PIE} indicates the most representative numerical expression of service requestor's opinion
2) En_{PIE} determines the range of testimonies forming *PIE*, i.e., *PIE* consistency
3) He_{PIE} reflects whether testimonies diverge from normal behavior, i.e., *PIE* coherency

Accordingly, when a *UH* service is requested, a cloud-based mechanism accumulates patient's group therapy colleagues' *PIE*s, stored in their User Profiles [30]. The generated *R* follows $C_R(Ex_R, En_R, He_R)$ representation, where:

1) Ex_R denotes expectation of testimonies distribution in *R*
2) En_R defines dispersion range of gathered testimonies, i.e., *R* consistency
3) He_R expresses accumulated testimonies diversion from Gaussian distribution, i.e., *R* coherency

Cloud theory, by enabling testimonies deviation and distribution abnormality to be quantified, provides a comprehensive representation of trust information sources [15]. In parallel, facilitates the expression of malicious attacks impact on R [30]. Although malicious attacks mainly affect En_R, the undercover by generating slightly false testimonies influence on He_R. In parallel, collusive behavior introduces additional abnormalities on testimonies distribution which can be detected with the use of He_R.

IV. Proposed Trust Model

In this paper, Trust Model is proposed to be deployed on *ACIS* that estimates $TV \in [0, 1]$ via a cloud (i.e., fuzzy-probabilistic) inference adaptable to trust information sources consistency and coherency. The adoption of cloud theory on linguistic inference implementation enables qualitative-quantitative intermapping of inputs and outputs to be accomplished in probabilistic terms. Hence, cloud inference becomes advantageous for reasoning under uncertainty [31].

The proposed *ACIS* takes as inputs $C_{PIE}(Ex_{PIE}, En_{PIE}, He_{PIE})$ and $C_R(Ex_R, En_R, He_R)$ where Ex_{PIE} and Ex_R are utilized for *TV* estimation while the pairs (En_{PIE}, He_{PIE}) and (En_R, He_R) are exploited as weighting means. As shown in Fig. 2, *ACIS* is a four-layer architecture, materializing a set of *If-Then* rules. *ACIS* architecture is analyzed considering the

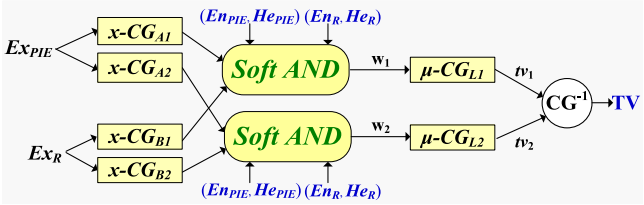

Fig. 2. Block diagram of the proposed Adaptable Cloud Inference System.

following two *If-Then* rules example:

$$\begin{aligned} &IF\ (patient's\ opinion\ is\ A_1)\ AND \\ &(acquaintances'\ opinion\ is\ B_1) \\ &THEN\ (trustworthiness\ is\ L_1) \\ &IF\ (patient's\ opinion\ is\ A_2)\ AND \\ &(acquaintances'\ opinion\ is\ B_2) \\ &THEN\ (trustworthiness\ is\ L_2) \end{aligned} \tag{2}$$

The variables Ex_{PIE}, Ex_R and *TV* constitute the most representative numerical expression of concepts "patient's opinion", "acquaintances' opinion" and "trustworthiness" which are assumed, in this example, to be specified by linguistic terms $A = \{A_i, i = 1, 2\}$, $B = \{B_j, j = 1, 2\}$ and $L = \{L_k, k = 1, 2\}$, respectively.

Although ACIS takes as inputs Ex_{PIE} and Ex_R, it exploits linguistic terms. Hence, each introduced crisp value (e.g., Ex_{PIE}) is mapped into a linguistic term (e.g., A_1) via a *x*-conditional Cloud Generator (*x-CG*) algorithm incorporating the corresponding membership cloud (e.g., $C_{Ai}(Ex_{Ai}, En_{Ai}, He_{Ai})$). Essentially, *x-CG* algorithms materialize rules antecedent part (e.g., IF (*personal opinion is A1*)) as follows:

$$\begin{aligned} \mu_{Ai}(Ex_{PIE}) &= \exp\left[-\frac{(Ex_{PIE} - Ex_{Ai})^2}{2{En'_{Ai}}^2}\right], \\ En'_{Ai} &\sim N(En_{Ai}, {He_{Ai}}^2),\ i = 1, 2 \\ \mu_{Bj}(Ex_R) &= \exp\left[-\frac{(Ex_R - Ex_{Bj})^2}{2{En'_{Bj}}^2}\right], \\ En'_{Bj} &\sim N(En_{Bj}, {He_{Bj}}^2),\ j = 1, 2 \end{aligned} \tag{3}$$

The produced $\mu_{Ai}(Ex_{PIE}), \mu_{Bj}(Ex_R) \in [0, 1]$ are certainty degrees denoting whether the corresponding crisp input (e.g., $Ex_{PIE} = 0.5$) belongs to a given linguistic term (e.g., A_1). In sense, 3 represents a fuzzy-probabilistic quantitative-qualitative transformation since certainty degree (e.g., $\mu_{Ai}(Ex_{PIE})$) is not a fixed value but a random number with stabilization tendency (e.g., $exp[-(Ex_{PIE} - Ex_{Ai})^2/2En_{Ai}^2]$).

Sequentially, the produced certainty degrees are organized into pairs as defined by *If-Then* rules (i.e., $(\mu_{A1}(Ex_{PIE}), \mu_{B1}(Ex_R))$ and $(\mu_{A2}(Ex_{PIE}), \mu_{B2}(Ex_R))$ according to 2). Each pair is introduced into an operator that produces rule activation degree ($w_p \in [0, 1]$) by materializing AND relation.

In the designed *ACIS*, a cloud relation operator, denoted as *soft AND*, is introduced. As shown in Fig. 3, *soft AND* is a *x-CG* algorithm that utilizes a 2-D cloud with $Ex_1 = Ex_2 = 1$ in order a rule to be fully activated (i.e., $w_n = 1$) when $\mu_{Ai}(Ex_{PIE}) = \mu_{Bj}(Ex_R) = 1$. Otherwise, w_n depends on a) the introduced certainty degrees as well as b) 2-D cloud entropies (En_1, En_2) and hyper-entropies (He_1, He_2), according to:

$$w_n = \exp\left[-\frac{(\mu_{Ai}(Ex_{PIE}) - 1)^2}{2{En'_1}^2} - \frac{(\mu_{Bj}(Ex_R) - 1)^2}{2{En'_2}^2}\right], \tag{4}$$

$$\text{where}\ \ En'_1 \sim N(En_1, {He_1}^2), En'_2 \sim N(En_2, {He_2}^2)$$

In sense, (En_1, He_1) and (En_2, He_2) determine contribution degree of $\mu_{Ai}(Ex_{PIE})$ and $\mu_{Bj}(Ex_R)$ into w_n production, respectively. In this paper, (En_1, He_1, En_2, He_2) parameters are proposed to be tuned by trust information sources consistency and coherency aiming on accurate *TV* estimation.

To meet the challenge of malicious attacks, the contribution degree of $\mu_{Bj}(Ex_R)$ on w_n, i.e., En'_2, is proposed to be reduced as long as the values of (En_R, He_R) increase. However, En'_2 is a random number following $N(En_2, He_2^2)$. For that purpose, variance of the 2-D cloud on the associate dimension with *R* (i.e., $\sigma_2^2 = En_R^2 + He_R^2$), is exploited instead of En'_2. Thus, a) σ_2 is proposed to be strictly decreasing function of σ_R and b) the values (En_2, He_2) are proposed to change uniformly in respect to (En_R, He_R).

Assuming that σ_2 and σ_R are linearly related, the former requirement implies:

$$\sigma_2 = \alpha\sigma_R + \beta,\ \alpha < 0 \tag{5}$$

Since $\mu_{Bj}(Ex_R) \in [0, 1]$ and $Ex_2 = 1$ then $\sigma_2 \in [0, 1/3]$. Given that testimonies composing R are defined within [0, 1], the maximum σ_R is equal to 0.5/3 and may occur when $Ex_R = 0.5$. Under these restrictions, 5 is transformed into:

$$\left.\begin{aligned} 0 \le \sigma_2 &= \sqrt{{En_2}^2 + {He_2}^2} \le 1/3 \\ 0 \le \sigma_R &= \sqrt{{En_R}^2 + {He_R}^2} \le 0.5/3 \end{aligned}\right\} \xrightarrow{Eq.5} \sigma_2 = -2\sigma_R + \frac{1}{3} \tag{6}$$

The latter requirement is mathematically expressed by:

$$\frac{He_2}{En_2} = \frac{He_R}{En_R} \tag{7}$$

Combining (6) and (7), En_2 and He_2 are given by:

$$En_2 = En_R\left(-2 + \frac{1}{3\sigma_R}\right), He_2 = He_R\left(-2 + \frac{1}{3\sigma_R}\right) \tag{8}$$

TV estimation is also possible to be manipulated by diverged and/or abnormally distributed testimonies composing *PIE*. To deal with that issue, $En'_1 \sim N(En_1, He_1^2)$ which is associated with $\mu_{Ai}(Ex_{PIE})$ is proposed to be adjusted in respect to

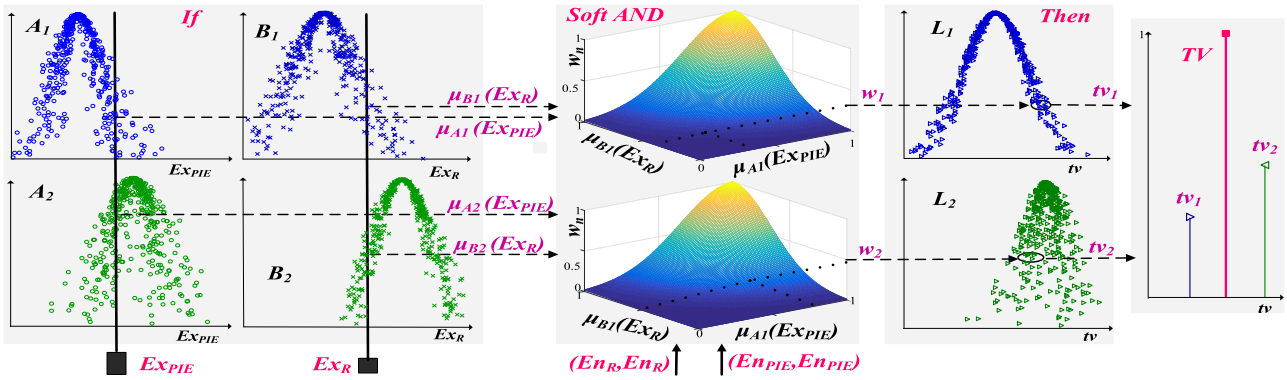

Fig. 3. Proposed Adaptable Cloud Inference System materializing the two If-Then rules example.

(En_{PIE}, He_{PIE}) as follows:

$$En_1 = En_{PIE}\left(-2 + \frac{1}{3\sigma_{PIE}}\right),$$
$$He_1 = He_{PIE}\left(-2 + \frac{1}{3\sigma_{PIE}}\right) \quad (9)$$

Equation 9 is emerged by following the aforementioned reasoning regarding (En_2, He_2) definition.

Essentially, the proposed design of *soft AND* ensures that $w_{\rm n}$ production is mainly influenced by the most consistent and coherent trust information source. In other words, *soft AND* performs an adaptable nonlinear weighting of trust information sources rather than testimonies filtering. In that way, the issue of outweighing benevolent testimonies, under complex malicious attacks, is avoided. Furthermore, the exploitation of cloud representation on *soft AND* tuning enables malicious attacks to be faced without the need of complex linearization or learning techniques.

On the next stage of *ACIS*, the produced $w_{\rm n}$ is introduced into a μ-conditional Cloud Generator $(\mu - CG)$ materializing rule consequent part (e.g., *THEN trustworthiness is* L_1). Each $\mu - CG$ algorithm incorporates a membership cloud, i.e., $C_{Lk}(Ex_{Lk}, En_{Lk}, He_{Lk})$, representing the linguistic term L_k posed by the associate rule. Thus, $\mu - CG$ algorithm derives a cloud drop (tv_n) from the corresponding membership cloud (C_{Lk}) under the perspective of rule activation degree (w_n). Namely:

$$tv_n = Ex_{Lk} \mp En'_{Lk}\sqrt{-2\ln(w_n)},$$
$$En'_{Lk} \sim N\left(En_{Lk}, {He_{Lk}}^2\right) \quad (10)$$

Essentially, tv_n selection from the linguistic term L_k is a stochastic process dependable on w_n. In 10, minus (plus) is applied when both Ex_{PIE} and Ex_R activate rising (falling) edges of corresponding C_{Ai} and C_{Bj}, otherwise the $\mu - CG$ algorithm produces two cloud drops.

As shown in Fig. 2, the generated cloud drops (i.e., tv_n) are introduced into a Backward CG (CG^{-1}) algorithm that produces *TV* as follows:

$$TV = \frac{1}{N}\sum_{n=1}^{N} tv_n \quad (11)$$

In *ACIS*, w_n significantly determines tv_n production and consequently *TV* estimation, therefore adaptable *soft AND* is the cornerstone of the proposed Trust Model robustness.

V. Simulation Results

The proposed Trust Model is validated in terms of accuracy and robustness via a set of simulations conducted within MATLAB environment, since the given paper focuses on *TV* estimation process modeling rather than Trust Model implementation environment. The basic structure of simulations conducted within MATLAB, is demonstrated in Fig. 4. Particularly, simulations are based on the widely utilized Epinions dataset [1] including a large number of timestamped 5-scale testimonies for category providers. Epinions data are mapped into [0, 1] (e.g., "3"→[0.4, 0.6]) with the use of 5 uniform distributions. PIE is formulated by considering a user at given timestamp as service requestor. Thus all his/her past testimonies are exploited for $C_{PIE}(Ex_{PIE}, En_{PIE}, He_{PIE})$ definition. *R* constitution is based on requestor's trust network, as defined within Epinions. Hence, $C_R(Ex_R, En_R, He_R)$ is calculated in respect to a subset of testimonies referring to a given category provider.

Malicious attacks are simulated by assigning $N(\lambda Ex_R, \kappa\sigma)$ to $p_m = \{10, 20, 40, 50\}\%$ of testimonies composing *R*. Assuming $\sigma = 0.01$, $\kappa = 1, 3$ express collusive and autonomous attacks, respectively. In case of undercover attack $\lambda = (Ex_R \pm En_R)/Ex_R$, otherwise $\lambda = (Ex_R \pm 4En_R)/Ex_R$.

ACIS implementation is based on 9 *If-Then* rules which are defined via simulation. The employed membership clouds, depicted in Fig. 5, are defined by applying to clean testimonies a Gaussian mixture algorithm customized for cloud theory [31]. Clean testimonies are, a priori, organized into linguistic concepts expressing 'patient's opinion', 'acquaintances opinion' and 'trustworthiness'.

Trust Models main objective is to estimate ground truth, exploiting partial knowledge of trust information sources. Ground

1.www.trustlet.org/epinions.html.

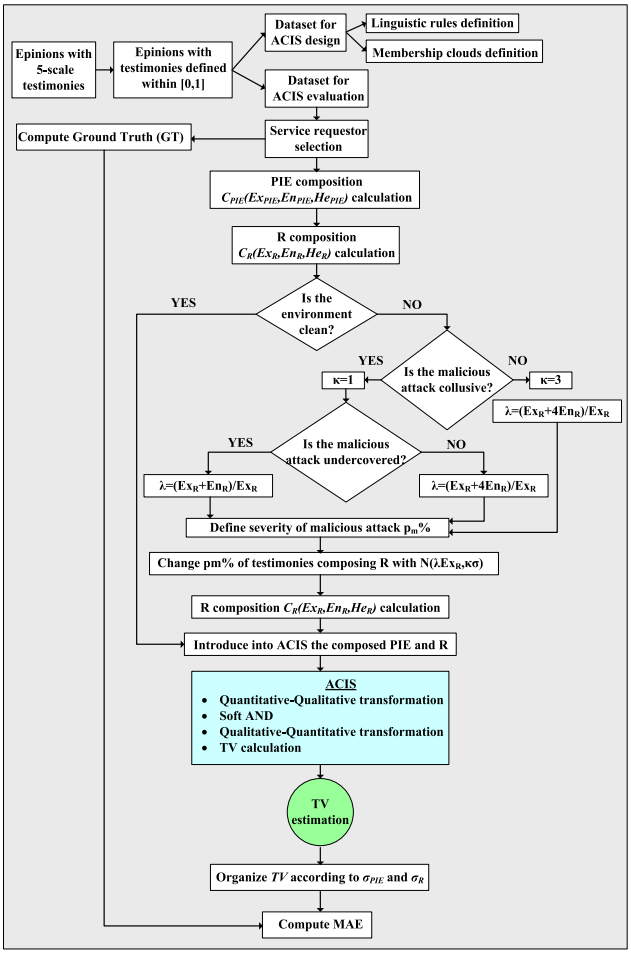

Fig. 4. Flowchart of simulation process conducted within MATLAB environment.

truth is defined as the mean value of all testimonies generated for a given category provider at a given timestamp. Thus, the proposed Trust Model is evaluated via mean absolute error (*MAE*) of *ACIS* output (TV_m) from ground truth (GT_m), under *M* different service requests with common σ_{PIE} and σ_R, namely:

$$MAE = \frac{1}{M}\sum_{m=1}^{M}|TV_m - GT_m| \tag{12}$$

Although *MAE* provides concrete information about Trust Model performance, a more comprehensive evaluation also includes investigation of discrimination capability between the trustworthy and the untrustworthy (*UH*) Providers with the use of the following metrics:

1) False Positive Rate (*FPR*) is the ratio of the wrongly estimated (*UH*) Providers as untrustworthy to the actual trustworthy (*UH*) Providers.
2) True Positive Rate (*TPR*) calculated by dividing the number of correctly estimated (*UH*) Providers as untrustworthy by the total number of actual untrustworthy (*UH*) Providers.

Given that $TV \in [0,1], TV = 0.5$ is considered as trustworthiness threshold. Therefore, a $TV > 0.5\,(TV < 0.5)$ declares a (*UH*) Provider which is estimated as trustworthy (untrustworthy). Accordingly, since testimonies are also defined within the range [0, 1], the actually trustworthy (untrustworthy) (*UH*) Providers have ground truth higher than *0.5* (lower than *0.5*).

Trust Model accuracy and robustness is evaluated via a comparative study based on 1) a linear Trust Model incorporating similarity weighing [23] and 2) a probabilistic inference Trust Model exploiting credibility as weighting mean [24]. Since comparative study aims on assessing Trust Models performance, MATLAB is exploited as simulation environment and Epinions dataset as evaluation basis. It is important to notice that tunable parameters of the aforementioned Trust Models are regulated via training process, in contrast to the proposed *ACIS*. Furthermore, optimal weights are assigned to similarity components utilizing linear Trust Model, as defined in [23].

Some distinct results of the conducted simulations indicating the proposed Trust Model effectiveness are demonstrated in following.

A. Feasibility

Initially, clean trust information sources are introduced into the proposed Trust Model in order the adopted mathematical background for TV estimation, to be evaluated. According to simulations results of Fig. 6, the introduced *ACIS* implementation enables TV to be estimated within clean environment with $MAE \leq 0.035$. Although such a result is an indicative that the combination of fuzzy-probabilistic reasoning along with the proposed weighting method (i.e., *ACIS*) is an efficient materialization, the proposed Trust Models performance is assessed via a comparative study. Simulations results of Table I demonstrate that the proposed *ACIS* implementation permits *TV* estimation to be performed within clean environment with 52% lower *MAE* in respect to linear Trust Model. Such a result verifies the theoretical claim that linear is rather than a sufficient modeling for *TV* estimation process due to inherited complexity and uncertainty. In that case low performance is also a matter of weighting since the adopted similarity weighting method is based on the assumption that PIE is closer to ground truth and thus R is weighted in accordance to how similar it is to PIE. However, the fact that two trust information sources are similar does not necessarily implies that they are close to ground truth. In parallel, *ACIS* materialization permits *TV* to be estimated with 40% higher accuracy compared to probabilistic inference materialization. Such a result proves that fuzzy-probabilistic reasoning provides more comprehensive modeling of *TV* estimation compared to stochastic approach of probabilistic inference.

B. Robustness

The proposed *soft AND* design enables enhanced estimation accuracy to be preserved even in case of malicious attacks. This is accomplished by tuning *soft AND* activation area (i.e., area wherein $w_n >> 0$). As indicated in Fig. 7, 29*8/–D cloud activation area is extended as long as En_{PIE} and En_R decrease and especially towards the dimension of the most consistent trust

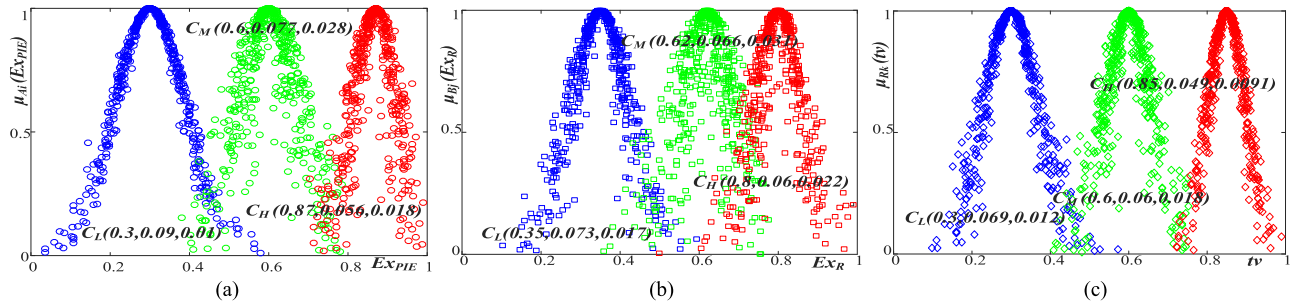

Fig. 5. Simulation results of membership clouds employed by the proposed Adaptable Cloud Inference System for (a) Personal Interaction Experience, (b) Reputation and (c) Trustworthiness qualitative-quantitative transformation.

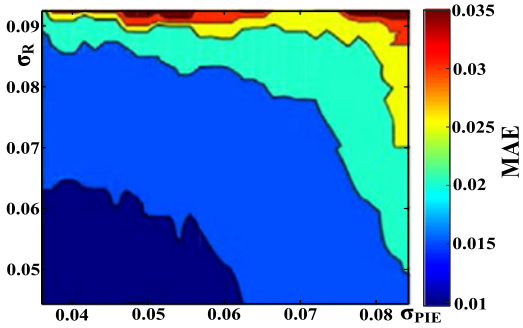

Fig. 6. Simulation results of mean absolute error (MAE) in respect to variance of PIE (σ_{PIE}) and R (σ_{R}), concerning TV estimation performing the proposed ACIS within clean environment.

TABLE I
SIMULATION RESULTS OF COMPARATIVE STUDY CONCERNING TV ESTIMATION ACCURACY

Trust Models	Upper limit of MAE
Linear implementation – similarity weighting [23]	0.073
Probabilistic inference implementation – credibility-weighting [24]	0.058
ACIS	0.035

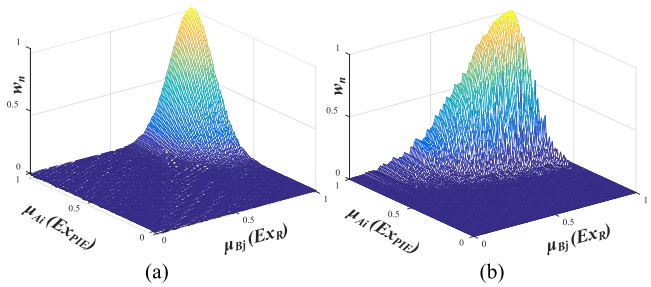

Fig. 7. Simulation results of 2-D cloud materializing soft AND operator in case that (En_{PIE}, He_{PIE}) and (En_R, He_R) are equal to a) (0.1,0.01), (0.08,0.009) and b) (0.07,0.012), (0.03,0.024), respectively.

information source. In parallel, 2-D cloud roughness depends on values of He_{PIE} and He_R. In that way, contribution of incoherent trust information source on *TV* estimation is more probable to deviate from 2-D cloud stabilization tendency.

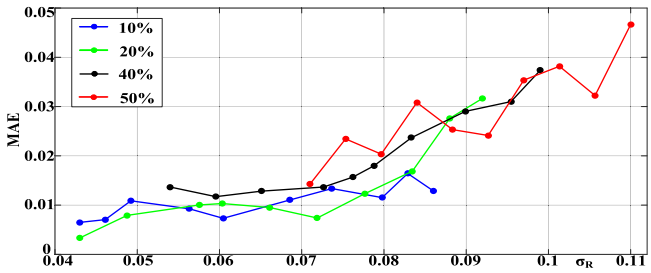

Fig. 8. Simulation results of MAE in respect to R variance (σ_{R}) in case that undercover malicious attacks affect $p_m = \{10, 20, 40, 50\}\%$ of R testimonies.

Robustness of the proposed Trust Model is evaluated via *MAE* in respect to σ_R while p_m of false testimonies in *R* changes parametrically. Since robustness is mainly a matter of trust information sources weighting, such an investigation permits the effectiveness of the proposed *soft AND* operator, exploiting coherency and consistency, to be evaluated. To focus on malicious attacks, in the conducted simulations consistent and coherent *PIE*s are utilized.

Undercover malicious attacks that generate slightly false testimonies constitute the first case study. As presented in Fig. 8, *TV* is estimated with $MAE < 0.05$ under this complex malicious attack. In contrast to the reported Trust Models, *ACIS* adaptability on coherency, expressing abnormality on testimonies distribution, apart from consistency of trust information sources enables such a result to be achieved. This is also accomplished because false testimonies' filtering is avoided on the proposed Trust Model implementation.

In sequence, the proposed Trust Model robustness against collusive malicious attacks is examined. According to simulation results of Fig. 9, *TV* estimation accuracy of *ACIS* is comparable to that achieved for clean environment, although *R* is under $p_m = \{10, 20\}\%$ collusive attack. Large scale malicious attacks are also effectively faced since $MAE \leq 0.11$ is achieved for $p_m = 50\%$. However, a comparative study with the aforementioned [23] and probabilistic inference [24] Trust Models verifies *ACIS* enhanced robustness (i.e., 55% on average lower *MAE*). As shown in Fig. 10, under $p_m = \{10, 20\}\%$ collusive attacks the proposed Trust Model performs *TV* estimation with 53% lower MAE in respect to the linear Trust Model. Since linear Trust Model exploits similarity as weighting mean, such

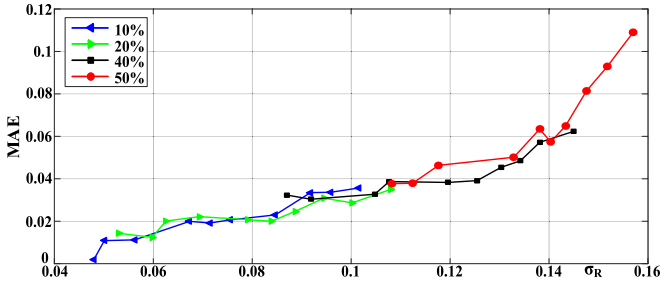

Fig. 9. Simulation results of *MAE* in respect to *R* variance (σ_{R}) that collusive malicious attacks affect $p_m = \{10, 20, 40, 50\}\%$ of R testimonies.

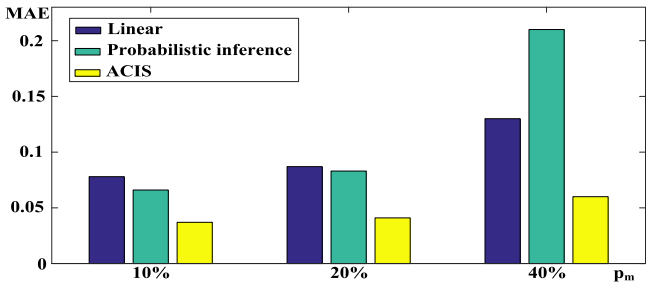

Fig. 10. Simulation results of *MAE* providing Trust Models deployed on linear, probabilistic inferences and *ACIS* schemes under collusive malicious attacks of $p_m = \{10, 20, 40\}\%$ severity.

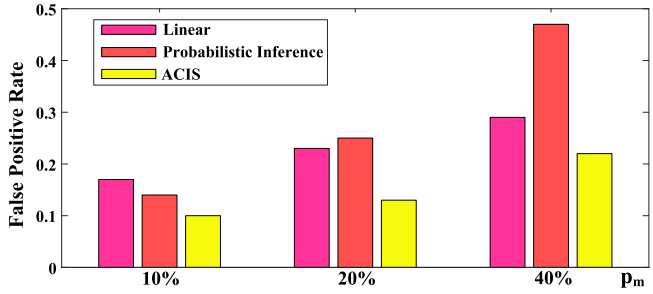

Fig. 11. Simulation results of False Positive Rate (*FPR*) achieving linear, and probabilistic inference Trust Models along with the proposed *ACIS* under collusive malicious attacks of $p_m = \{10, 20, 40\}\%$ severity.

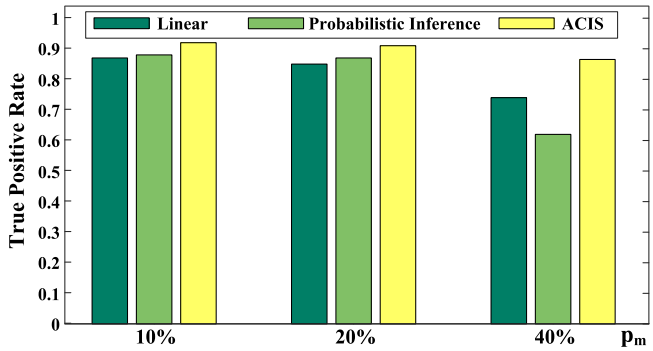

Fig. 12. Simulation results of True Positive Rate (*TPR*) achieving linear, and probabilistic inference Trust Models along with the proposed *ACIS* under collusive malicious attacks of $p_m = \{10, 20, 40\}\%$ severity.

a result shows that similarity rather than reveals malicious behavior even though an optimized weighting scheme is adopted. However, the proposed Trust Model also achieves to estimate *TV* under $p_m = \{10, 20\}\%$ with 47% higher accuracy in respect to probabilistic inference Trust Model. Since consistency is the equivalent of coherency, such a result shows that the utilization of coherency as additional weighting mean has a positive impact on the achievement of robustness against malicious attacks. The utilization of coherency-consistency into an innovative weighting method with geometrical background (i.e., *soft AND*) enables the proposed Trust Model to be robust even against large scale (i.e., $p_m = 40\%$) collusive malicious attacks, as indicated in Fig. 10. Simulation results also verify that complex malicious attacks can mislead probabilistic threshold schemes, as that incorporated into the investigated probabilistic inference Trust Model.

Comparative study is extended by evaluating Trust Models discrimination capability between the trustworthy and untrustworthy providers under different severity (p_m) of collusive attacks. Simulation results of Fig. 11 indicate that the proposed Trust Model has almost 50% fewer false positives in respect to the investigated linear Trust Model, under $p_m = 10\%$ collusive attacks. As malicious attack severity increases to 20%, *TPR* of the investigated Trust Models is slightly reduced, as depicted in Fig. 12. Under the same conditions, *FPR* of both linear and probabilistic inference Trust Models are significantly affected in contrast to the proposed *ACIS*. This is enabled by the enhanced robustness providing the innovative weighting method to the proposed Trust Model. Even under the highly misleading large scale $(p_m = 40\%)$ collusive attacks, the proposed Trust Model robustness permits untrustworthy providers to be determined with $TPR = 0.87$. On the contrary, discrimination capability of the other two investigated Trust Models is significantly deteriorated as shown in Fig. 11. Especially, the high *FPR* of probabilistic inference Trust Model declares vulnerability to large scale collusive attacks.

VI. Experimental Investigation

The proposed Trust Model is designed to cover the need of establishing a trustful background on patients-psychologists interactions taking place within a *UH* environment dedicated for anxiety disorders. Psychologists highlight that trustworthiness is key factor for patients' satisfaction and becomes a fundamental requirement for effective mental treatment. That theoretical claim is experimentally investigated by determining whether the adoption of the proposed Trust Model within a *UH* environment oriented on anxiety disorders is profitable. In detail, experimental investigation is conducted in cooperation with Medicine School of Democritus University of Thrace and private Psychological Centre in Alexandroupolis. Main objective of the conducted experiment is to record patients' satisfaction from interaction with a psychologist who are selected a) randomly and b) in terms of trustworthiness estimated by the proposed Trust Model. It is important to notice that criteria of availability and familiarity are the same for all subjects while cost criterion is out of context. On that basis, satisfaction rate is calculated

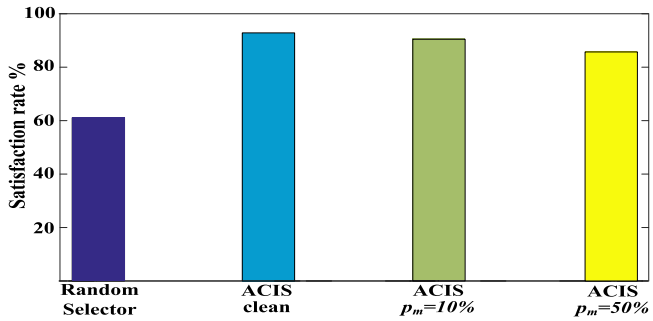

Fig. 13. Experimental results of patients' satisfaction rate after interacting with psychologists which have been selected randomly and with the use of the proposed Trust Model within clean environment and under the influence $p_m = \{10, 50\}\%$ collusive malicious attacks.

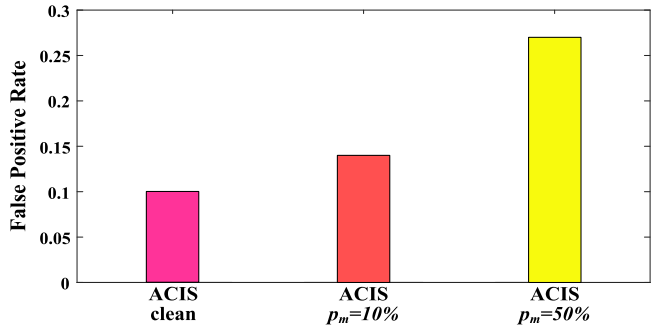

Fig. 14. Experimental results of False Positive Rate (*FPR*) achieving the proposed *ACIS* within clean environment and under collusive malicious attacks of $p_m = \{10, 50\}\%$ severity.

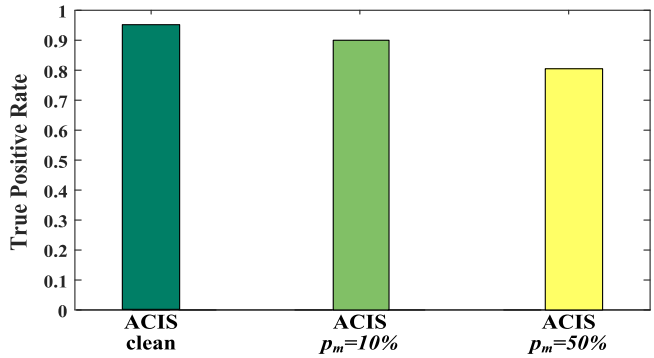

Fig. 15. Experimental results of True Positive Rate (*TPR*) achieving the proposed *ACIS* within clean environment and under collusive malicious attacks of $p_m = \{10, 50\}\%$ severity.

as the ratio of successful interactions to the total number of conducted interactions.

In detail, 27 subjects (40% male and 60% female), aged 22-34 years old, facing anxiety issues volunteered to participate. Subjects are under the supervision of cooperating Psychological Centre and thus they are familiar with all psychologists participating in the experiment. Within a period of 5 weeks, subjects participate into group therapy or a personal session, via a teleconference platform. After the completion of each session, subjects are requested to declare their satisfaction via a 10-level scale.

During the first 3 weeks, subjects proceed into group therapy session of 7 participants, three times per week. The supervisor psychologist of group therapy changes every week. During the last 2 weeks, subjects perform personal sessions with a selected psychologist, 3 times per week. The subjects are split into 2 groups of 6 and 21 participants, respectively. Participants of first group interact with randomly selected psychologists. On the contrary, subjects of the second group interact with psychologists selected under trustworthiness perspective.

Testimonies acquired within the first 3 weeks are exploited for *PIE* and *R* constitution. Especially, *R* is formulated on the basis of group therapy participants. However, false testimonies are highly possible to be generated, due to patients' extremely benevolent or strict evaluating behavior. To examine this case, the second group is further divided into 3 subgroups of 7 subjects. Into second and third subgroups, the 10% and 50% of testimonies composing *R* are replaced with false. Psychologists' trustworthiness is estimated by introducing into ACIS the emerged *PIE* and *R*. Psychologist with the highest *TV* is selected for interaction.

Exploiting subjects' testimonies regarding personal sessions, satisfaction rate is calculated. The presented in Fig. 13 experimental results indicate that trust-oriented psychologist selection significantly ameliorate satisfaction rate. Even in case that R includes false testimonies, trust-based selection ensures 27% on average greater satisfaction rate in respect to random selection.

The acquired testimonies are also exploited for experimentally assessing the proposed Trust Model discrimination capability between the trustworthy and the untrustworthy *UH* Providers. This is accomplished with the use of *TPR* and *FPR* metrics as defined in Section V. Additionally, the definition of actual and estimated trustworthy or untrustworthy *UH* Providers, demonstrated in Section V, are also adopted into experimental investigation. However, the term 'untrustworthy' does not declare that a psychologist is incapable or insufficient to perform a treatment but his/her pattern does not comply with patient's personality and point of view.

Experimental investigation based on *FPR* and *TPR* permits to evaluate on what degree the proposed Trust Model serves its purpose, namely patients' assistance to discover and select trustworthy *UH* Providers for interactions. Random selector has by default equal probability to recommend for interaction either a trustworthy or an untrustworthy *UH* Provider. However, since random selector is considered as evaluation baseline, the experimental results of *FPR* and *TPR* of Figs. 14 and 15 indicate that the proposed Trust Model has high discrimination capability. In particular, the significantly high *TPR* achieved by the proposed *ACIS* materialization declare that the actual untrustworthy psychologists are precisely determined, when *TV* is estimated within clean environment. Discrimination capability is preserved even though *R* is affected by $p_m = 10\%$ collusive malicious attacks, since *FP*R remains lower to 0.15. Furthermore, the proposed Trust Model achieves a *TPR* greater than 0.8 although 50% of *R* testimonies are replaced with erroneous. The presented experimental results of *FPR* and *TPR* justify the

high patients' satisfaction rate under different conditions observed in experimental results of Fig. 13.

VII. Conclusion

The necessity of establishing trustful background on patient-psychologist interactions taking place within *UH* environment is covered by assisting patients to discover and select trustworthy *UH* Providers for interaction. This is accomplished by the proposed Trust Model that a priori to service delivery estimates *UH* Providers trustworthiness, in terms of *TV*s, by exploiting *PIE* and *R*. To meet the challenge of accurate and robust *TV* estimation, the introduced Trust Model is proposed to be materialized via an innovative *ACIS*. Especially, the adoption of cloud theory that comprehensively deals with uncertainty, enables *TV* to be estimated via an advantageous fuzzy-probabilistic (i.e., cloud) reasoning. In parallel, an innovative weighting method of *PIE* and *R* is developed on the basis of a cloud relation operator (*soft AND*) which is proposed to be tuned by trust information sources consistency and coherency. Apart from testimonies dispersion range, the utilization of coherency as additional weighting mean into the proposed geometrical weighting scheme significantly contribute into Trust Model amelioration performance. According to the conducted comparative study, the introduced *ACIS* implementation enables accuracy of *TV* estimation within clean environment to be enhanced about 45.5% on average. Accurate TV estimation is preserved even in case of undercover attacks as indicated by $MAE \leq 0.05$. Beyond the proposed Trust Model outperformance under collusive malicious attacks, the enhanced robustness providing against large scale attacks is of most significance. Especially, *ACIS* enables *TV* to be estimated with 62% on average higher accuracy under $p_m = 40\%$ collusive attacks in respect to the investigated Trust Models. The innovative features of *ACIS* also facilitate efficient discrimination between trustworthy and untrustworthy (*UH*) Providers within clean environment and under malicious attacks, as both simulation and experimental results verify. Particularly, under large scale collusive attacks the proposed Trust Model not only achieves significantly lower *FPR* in respect to probabilistic inference Trust Model but also preserves *TPR* greater than *0.8*. Finally, the presented experimental investigation proves that the proposed Trust Model serves the purpose of ensuring high satisfaction level for patients interacting with psychologists within *UH* environment.

References

[1] B. Saha, T. Nguyen, D. Phung, and S. Venkatesh, "A framework for classifying online mental health-related communities with an interest in depression," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 4, pp. 1008–1015, Jul. 2016.

[2] E. Garcia-Ceja, V. Osmani, and O. Mayora, "Automatic stress detection in working environments from smartphones' accelerometer data: A first step," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 4, pp. 1053–1060, Jul. 2016.

[3] A. Hernando *et al.*, "Inclusion of respiratory frequency information in heart rate variability analysis for stress assessment," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 4, pp. 1016–1025, Jul. 2016.

[4] M. E. Larsen, T. W. Boonstra, and P. J. Batterham, "We feel: Mapping emotion on twitter," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 4, pp. 1246–1252, Jul. 2015.

[5] P. Pandey, E. Lee, and D. Pompili, "A distributed computing framework for real-time detection of stress and of its propagation in a team," *IEEE J. Biomed. Health Informat.*, vol. 20, no. 6, pp. 1502–1512, Nov. 2016.

[6] Q. Xu, T. L. Nwe, and C. Guan, "Cluster-based analysis for personalized stress evaluation using physiological signals," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 1, pp. 275–281, Jan. 2015.

[7] T. C. Panagiotakopoulos, D. P. Lyras, M. Livaditis, K. N. Sgarbas, G. C. Anastassopoulos, and D. K. Lymberopoulos, "A contextual data mining approach toward assisting the treatment of anxiety disorders," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 3, pp. 567–581, May 2010.

[8] M. A. Fengou, G. Mantas, D. Lymberopoulos, N. Komninos, S. Fengos, and N. Lazarou, "A new framework architecture for next generation e-health services," *IEEE J. Biomed. Health Informat.*, vol. 17, no. 1, pp. 9–18, Jan. 2013.

[9] J. Andreu-Perez, C. C. Y. Poon, R. D. Merrifield, S. T. C. Wong, and G. Z. Yang, "Big data for health," *IEEE J. Biomed. Health Informat.*, vol. 19, no. 4, pp. 1193–1208, Jul. 2015.

[10] E. McGinnis *et al.*, "Movements indicate threat response phases in children at-risk for anxiety," *IEEE J. Biomed. Health Informat.*, to be published.

[11] Q. Li, Y. Xue, L. Zhao, J. Jia, and L. Feng, "Analyzing and identifying teens stressful periods and stressor events from a microblog," *IEEE J. Biomed. Health Informat.*, to be published.

[12] M. Hoogendoorn, T. Berger, A. Schulz, T. Stolz, and P. Szolovits, "Predicting social anxiety treatment outcome based on therapeutic email conversations," *IEEE J. Biomed. Health Informat.*, to be published.

[13] G. Athanasiou, M. A. Fengou, A. Beis, and D. Lymberopoulos, "A novel trust evaluation method for Ubiquitous Healthcare based on cloud computational theory," in *Proc. 36th IEEE Annu. Int. Conf. Eng. Med. Biol. Soc.*, Chicago, IL, USA, 2014, pp. 4503–4506.

[14] X. Yang, Y. Guo, and Y. Liu, "Bayesian-inference-based recommendation in online social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 642–651, Apr. 2013.

[15] G. Athanasiou, M. A. Fengou, A. Beis, and D. Lymberopoulos, "A trust assessment mechanism for ubiquitous healthcare environment employing cloud theory," in *Proc. 37th IEEE Annu. Int. Conf. Eng. Med. Biol. Soc.*, Milan, Italy, 2015, pp. 1405–1408.

[16] J. Matysiewicz and S. Smyczek, "Consumer trust— Challenge for E-healthcare," in *Proc. 4th Int. Conf. Cooperation Promotion Inf. Resour. Sci. Technol*, Beijing, China, 2009, pp. 333–338.

[17] T. Lu, H. Chen, Y. Xu, and C. Zhang, "Internet usage, physician performances and patient's trust in physician during diagnoses: Investigating both pre-use and not-use internet groups," in *Proc. 49th Hawaii Int. Conf. Syst. Sci.*, Koloa, HI, USA, 2016, pp. 3189–3198.

[18] M. Silic, G. Delac, and S. Srbljic, "Prediction of atomic web services reliability for QoS-aware recommendation," *IEEE Trans. Serv. Comput.*, vol. 8, no. 3, pp. 425–438, May/Jun. 2015.

[19] B. Li, L. Liao, H. Leung, and R. Song, "PHAT: A preference and honesty aware trust model for web services," *IEEE Trans. Netw. Serv. Manage.*, vol. 11, no. 3, pp. 363–375, Sep. 2014.

[20] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

[21] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1164–1175, Nov. 2012.

[22] E. Ayday and F. Fekri, "Iterative trust and reputation management using belief propagation," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 3, pp. 375–386, May/Jun. 2012.

[23] I. R. Chen, J. Guo, and F. Bao, "Trust management for SOA-based IoT and its application to service composition," *IEEE Trans. Serv. Comput.*, vol. 9, no. 3, pp. 482–495, May/Jun. 2016.

[24] X. Wang, L. Liu, and J. Su, "RLM: A general model for trust representation and aggregation," *IEEE Trans. Serv. Comput.*, vol. 5, no. 1, pp. 131–143, Jan./Mar. 2012.

[25] Y. Yao, H. Tong, X. Yan, F. Xu, and J. Lu, "Multi-aspect + transitivity + bias: An integral trust inference model," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 7, pp. 1706–1719, Jul. 2014.

[26] X. Wu, B. Cheng, and J. L. Chen, "Collaborative filtering service recommendation based on a novel similarity computation method," *IEEE Trans. Serv. Comput.*, vol. 10, no. 3, pp. 352–365, May/Jun. 2017.

[27] S. Wang, Z. Zheng, Z. Wu, M. R. Lyu, and F. Yang, "Reputation measurement and malicious feedback rating prevention in web service recommendation systems," *IEEE Trans. Serv. Comput.*, vol. 8, no. 5, pp. 755–767, Sep./Oct. 2015.

[28] Y. Wang and L. Li, "Two-dimensional trust rating aggregations in service-oriented applications," *IEEE Trans. Serv. Comput.*, vol. 4, no. 4, pp. 257–271, Oct./Dec. 2011.

[29] H. K. Oh, S. W. Kim, S. Park, and M. Zhou, "Can you trust online ratings? A mutual reinforcement model for trustworthy online rating systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 45, no. 12, pp. 1564–1576, Dec. 2015.

[30] G. Athanasiou and D. Lymberopoulos, "A comprehensive reputation mechanism for ubiquitous healthcare environment exploiting cloud model," in *Proc. IEEE 38th Annu. Int. Conf. Eng. Med. Biol. Soc.*, Orlando, FL, USA, 2016, pp. 5981–5984.

[31] D. Li and Y. Du, *Artificial Intelligence With Uncertainty*. London, U.K.: Chapman & Hall, 2008.

[32] Z. Zhou, "Cognition and removal of impulse noise with uncertainty," *IEEE Trans. Image Process.*, vol. 21, no. 7, pp. 3157–3167, Jul. 2012.

[33] X. Han, Y. Yan, C. Cheng, Y. Chen, and Y. Zhu, "Monitoring of oxygen content in the flue gas at a coal-fired power plant using cloud modeling techniques," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 4, pp. 953–963, Apr. 2014.