

Developing a trust model using graph and ranking trust of social messaging system

Mostafa Heidarzadeh Kalahroudy, Kheirollah Rahsepar Fard, Yaghoob Farjami

Department of Computer Engineering and Information Technology, University of Qom, Qom, Iran

Article Info

Article history:

Received Jul 14, 2021

Revised Sep 2, 2022

Accepted Sep 26, 2022

Keywords:

Analytic network process

Graph

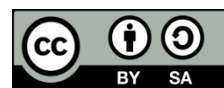
Trust pathways measure

Trusts model

ABSTRACT

Trust is an important issue in social interactions, especially in using cyberspace services. In this paper, a trust and evaluation model are proposed based on which the government can provide reliable services to users. The model is a distributed and hierarchical model. First, the number 12 trust criteria and the weight of these criteria were extracted using the analytical hierarchy process (AHP) and analytic network process (ANP) techniques. Second, to obtain the trust in the service examined, for each criterion, a graph of trusted entities is proposed. Then, a weighted graph with the number of trusted entities called trust pathways measure will be obtained. To test the model, the effect of the 12 criteria on three important evaluation factors over seven widely used social services was rated by three experts. The trust of each service was obtained, which was satisfactory as compared to a valid organizational evaluation. Finally, the correlation coefficient of this comparison was 70.37%, indicating that the results from this model were appropriate.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mostafa Heidarzadeh Kalahroudy

Department of Computer Engineering and Information Technology, University of Qom

Qom, Iran

Email: heydarzadeh.mostafa@yahoo.com

1. INTRODUCTION

Ensuring the observance of the rights of public users of various cyberspace services is the key issue and challenge in this study. A trust method and a monitoring system of public rights in a country is responsible for advising users to prevent violating their rights by the service providers. Therefore, there is a need for a comprehensive and verifiable model for assessing service providers that are competing with each other and, if necessary, providing corrective instructions to these companies. Moreover, the rating of different services will lead to prioritization and higher trust among their users.

The importance of this issue is to the extent that it has been addressed in the National Strategy for Trusted Identities in Cyberspace (NSTIC) document signed and announced by the President of the United States in 2011. This document provides a context for public and private sectors for cooperation to enhance the level of trust in the identities of individuals, organizations, networks, services, and tools in online exchanges. One of the strategic goals of this national document is that individuals and organizations use secure, efficient, easy, and collaborative identity solutions to achieve online services in a way that enhances trust, privacy, choice, and innovation. This document will be explained in the second section. Since the main topic of this study is the calculation of service trust and evaluation, further explanations have been made on this topic.

Trust is an integral component in many kinds of human interaction, allowing people to act under uncertainty and with the risk of negative consequences. Trust often refers to mechanisms to verify that the source of information is really who the source claims to be [1]. Trust management embodies the concept of

confidence between two nodes, i.e., trust between a trustee and a trustor [2]. Inaccurate trust estimation can allow a trustor to place false trust in a trustee (i.e., mistrust), leading to a betrayal by the trustee or losing opportunities with good collaborators [3]. The success of such attempts relies on the level of trust that members have with each other as well as with the service provider. Therefore, trust becomes an essential and important element of a successful social network [4]. Trust has many different aspects such as calculative, relational, emotional, institutional aspects of trust. When we talk about trust aspects, we consider a perspective from which we look at trust. This perspective often gives different semantics to trust [5].

Analytic network process (ANP) is generated from control hierarchies, clusters, nodes, the interrelationship among nodes and the interrelationship among clusters [2]. The ANP network contains clusters that are built on the criteria and elements that make up the sub criteria. Depending on the size, the system can include subsystems, and each subsystem is composed of elements. In the structure of the ANP, the decision issue has become a network structure with decision making criteria, goals, and remedies [6]. There is a mapping between the decision levels and the network structure elements used for the analysis network process [7], [8]. The innovations are the extraction of service measurement and evaluation indicators. The importance of the proposed method was due to the use of expert method and the transfer of knowledge and experiences of other countries or other regulatory agencies such as European Union (EU) general data protection regulation (GDPR), besides the existence of a trusted and real case in cyberspace as a case study was examined in this investigation.

In this research, in order to obtain the level of trust in a service, a hierarchical and networked two-level model has been proposed. At the first level of this model, trust indicators were first extracted and evaluated, and after performing the ANP, these indicators were weighted. In the second level, for each of the trust indicators, a weighted graph is proposed; each service receives a trust weight by entering into this graph and gaining trust in each index, by trusted entities in the network. Using this model, the complex network of cyberspace can be simulated as a weighted trust graph, in which each entity determines whether or not interact with its interaction party by examining its trust level. In section 2, the research background and studies related to this article will be addressed. In section 3, the proposed method, and in section 4, the test of the new formula will be discussed. Finally, in section 5 the case study has been discussed.

2. CONCEPTUAL BACKGROUND

Weighted sum is a popular technique to aggregate evidence. Many reputation systems [8] aggregate ratings or feedbacks using weighted sum such that raters with a higher reputation or transaction relevance have a higher weight. Ud-Din *et al* [9] used credibility (derived from quality of service [QoS] and social trust) as the weight associated with the recommendation or feedback provided by a rater for indirect trust aggregation [10] also used similarity (derived from social trust) as the weight for indirect trust aggregation.

From the network perspective, trust models can be divided into two types: those using a local approach that considers personal bias, and those using a global approach that considers all users' opinions. Graph-based models usually take the local approach. They can be scalar metrics, which cope with the setting where a source s is interested in a single target [11]. Based on how to cope with the trusted graph, graph-based trust models can be classified into two categories [12].

First, the graph simplification-based approach. As its name implies, this approach simplifies a trusted graph into multiple paths whose nodes or edges are disjointed with each other. It may also simplify a trusted graph into a directed series-parallel graph, which is an important concept in graph theory. Second, the graph analogy-based approach. Different from the preceding approach, this approach does not remove any nodes or edges from trusted graphs. Instead of simplification, it emulates the trusted graph by using other graphs.

Graph simplification-based models face the challenges of setting proper path length limitations and keeping evidence availability. Graph analogy-based models face the challenges of normalization and scalability. Moreover, all graph-based models face four common challenges: path dependence, trust decay, opinion conflict, and attack resistance [13].

In the NSTIC document, an identity ecosystem and a trust-based conceptual model have been defined. In this model, the information of each entity is divided into two categories: identity and attribute information. Entities include individuals, organizations, hardware, software, and data. As illustrated in Figure 1, there are two types of trusted centers in this model, identity provider that issues the confirmations of identity information of entities as shown in Figure 1(a) and attribute provider that issues the confirmations of the attribute information as shown in Figure 1(b). Since the information of the attributes is diverse, the certification centers can vary.

As shown in Figure 2, each entity obtains confirmation of presence in this ecosystem after receiving two identity and attribute confirmations by a relying party (RP). In addition, in this ecosystem, any product or

service provider that has the requirements of this ecosystem will be granted a confirmation called a Trustmark to be present in the ecosystem. Trustmark helps users in this model, including individuals and organizations, to make the proper and preferred choices in services provided in the identity ecosystem. The focus in the present study was to obtain attribute information confirmations, with trusted entities used in the proposed method in the network. The proposed model in this study can examine and validate different entities of this ecosystem for granting a Trustmark.

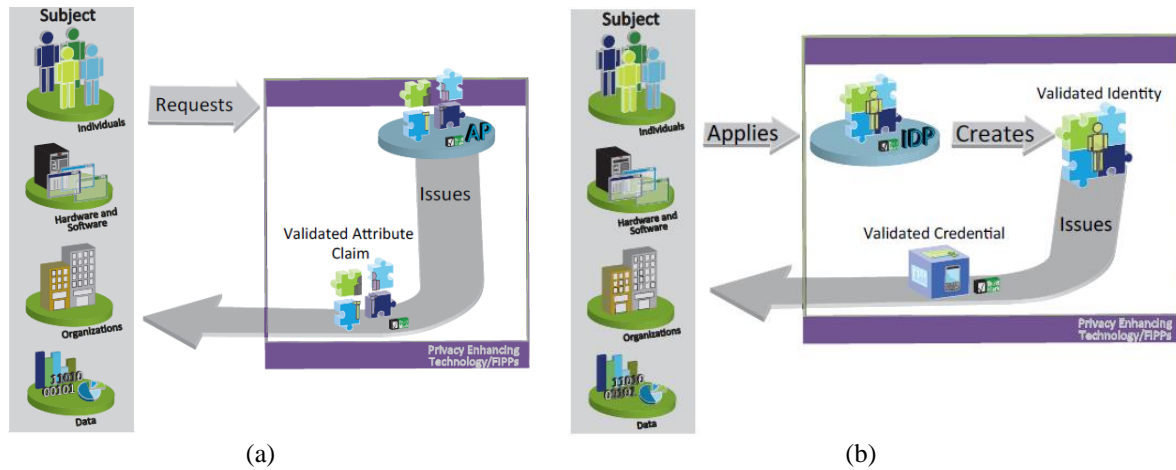


Figure 1. Two types of trusted centers in this model: (a) a subject obtains a validated attribute claim to use in online transactions on the left and (b) a subject obtains a validated credential to use in online transactions on the right

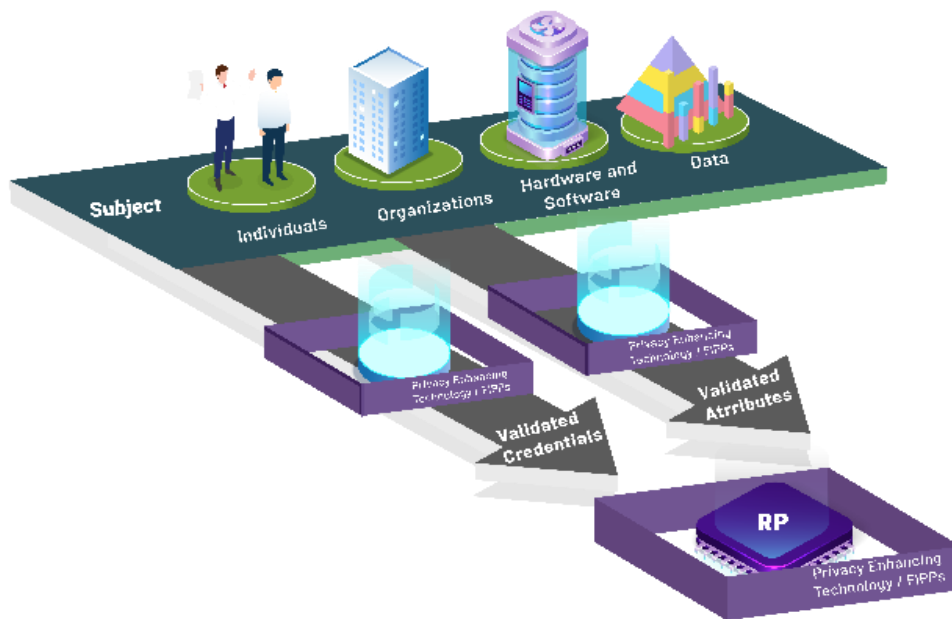


Figure 2. A subject supplies validated credentials and attribute claims to relying party to authorize an online transaction

To achieve the model, 26 trust criteria have been selected by reviewing books and articles as well as using experts' opinions. Then, opinions of seven experts were asked on the prioritization of the criteria according to a Likert-scale questionnaire and based on the Cronbach's alpha test, the average Cronbach's coefficient was obtained 0.893, and finally from the 26 criteria, 12 criteria had a value more than the average. To have proper prioritization and weighing, it seems necessary to note that the criteria are

interconnected as a network. To achieve this purpose, we used the network analysis method in this paper. To further investigate, the research model was explored for a case study in the field of social messaging services, and these services were prioritized according to the 12 trust criteria.

3. RESEARCH METHOD

Based on the conceptual framework in Figure 3, we propose a research model with two methods for evaluating trust. In addition, we propose this formula for evaluation of seven messaging agents. The key issue and challenge in this study was to ensure that the rights of public users of various cyberspace services are respected. To achieve this goal, in this study, a trust and evaluation model was proposed based on which the government can provide reliable services to users, and users use these services with more security.

In this paper, a two-level model was proposed to obtain the degree of trust in an entity as shown in Figure 3. The trust level for each indicator is calculated independently of other indicators. The level of trust in each indicator includes two parameters, the extent of confirmations of trusted entities in the network, and the degree of trust in these trusted entities. Trusted entities in the network are entities that can issue confirmations for the services examined by this model. As depicted in Figure 4, trusted entities and their number may differ relative to each of the trust indicators.

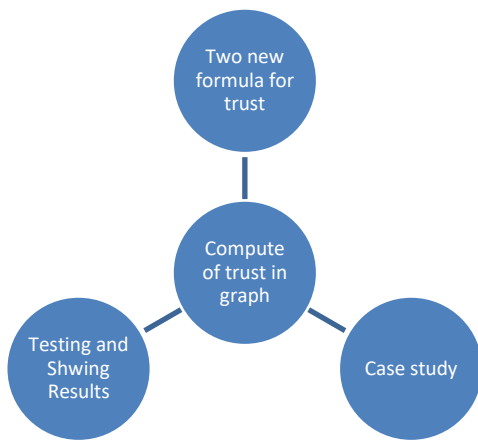


Figure 3. Research model

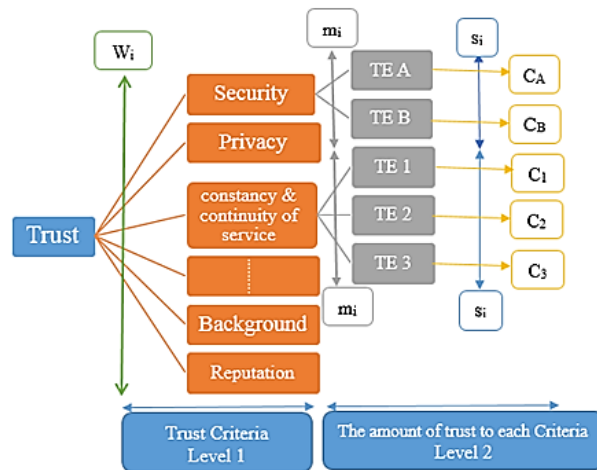


Figure 4. Two-level model of trust calculation (Level 1: weight of indicators and level 2: trust to each indicator)

In (1), the level of trust in each service (T), is obtained from Table 1 represents the effective parameters in calculating the amount of trust in the proposed model.

$$T = \sum_{i=1}^n W_{ik} * v_i \sum_{j=1}^{m_i} t_{ij} * t_{jk} , \text{ for each path } k, \tag{1}$$

where T is an amount of trust in a service, v_i is an amount of each service, w_{ik} is weight of each trust index and t_{ij} is weight of the confirmation obtained for each index in a service.

3.1. Instrument development (extraction of indicators and their weights)

As indicated in (1), at the elementary level, the extraction of trust indicators and the weight of each of them (W_i) were investigated. In the first step, it was necessary to obtain the trust indicators, and the method of extraction and weighting of the indicators included three steps; step 1: How extract trust criteria, step 2: choosing the analysis model and gathering the experts' opinions, and step 3: extracting and analyzing the weights of the criteria and proposing a model.

3.1.1. Step 1: how to extract trust criteria

The objective in this study was to provide an evaluation model and trust calculation to measure the amount of trust in each entity. We research the trust criteria in research papers or national strategic

documents of countries, for example National Strategy for Trusted Identities in Cyberspace (NSTIC) of United State of America [3], [8], [9], [14], [15]. Then, three scientific and professional experts, by taking into account measurability the criteria, classified them. Finally, 26 trust criteria were extracted. Note that the presented trust model has been designed for cyberspace. Therefore, the criteria for two levels, service provider and service requester, are established. The criteria for requesting a service user are reputation, position of requesting node, profit and value, responsibility, background, credit, similarity, certifiers, sensitivity of requesting subject. Furthermore, the criteria for service are security, privacy, profit and value, knowledge, resource sharing, credit, transparency and traceability, correction rate, reliability, scalability, evolvability and adaptability, constancy and continuity of service, auditing, redundancy, flexibility, compatibility, compliance with the standard. The extracted criteria, by questionnaire with Lick ret spectrum including odd numbers one till nine inserted. Seven experts were asked about the priorities of these criteria. The scientific experts are staff of Sharif, Amirkabir, Science and technology universities and professional's experts are manager or service provider in cyberspace. Answers of experts, with SPSS program, are evaluated and middle of evaluation is 6.242 and also Cronbach's alpha is 0.893. Twelve criteria are higher than middle, and the other criteria are deleted as shown in Table 1.

Table 1. Cronbach's alpha and the value of criteria

| Std. Deviation | Mean | | Std. Deviation | Mean | |
|----------------|--------|-----------|----------------|--------|----------|
| 1.37437 | 7.3329 | VAR000014 | 1.57359 | 8.1429 | VAR00001 |
| 0.94281 | 7.6657 | VAR000015 | 2.21108 | 5.6657 | VAR00002 |
| 1.90238 | 7.5714 | VAR000016 | 2.51661 | 6.0000 | VAR00003 |
| 2.76887 | 6.0000 | VAR000017 | 1.38013 | 7.2857 | VAR00004 |
| 2.42997 | 5.2857 | VAR000018 | 1.38013 | 6.7143 | VAR00005 |
| 2.22539 | 3.5714 | VAR000019 | 2.26779 | 6.1429 | VAR00006 |
| 2.54484 | 6.1429 | VAR000020 | 0.97590 | 2.4286 | VAR00007 |
| 1.57359 | 7.8571 | VAR000021 | 2.42997 | 5.2857 | VAR00008 |
| 1.06904 | 8.1429 | VAR000022 | 1.90238 | 6.4286 | VAR00009 |
| 2.74946 | 6.3571 | VAR000023 | 0.97590 | 7.5714 | VAR00010 |
| 2.76026 | 5.5714 | VAR000024 | 1.63299 | 5.0000 | VAR00011 |
| 2.00000 | 5.0000 | VAR000025 | 1.95180 | 5.8571 | VAR00012 |
| 2.92770 | 7.2857 | VAR000026 | 2.54484 | 6.1429 | VAR00013 |

3.1.2. Step 2: choosing the analysis model and gathering the experts' opinions

They are reputation, position of requesting node, profit and value, responsibility, background, credit, similarity, certifiers, sensitivity of requesting subject. Furthermore, the criteria for service area are security, privacy, profit and value, knowledge, resource sharing, credit, transparency and traceability, correction rate, reliability, scalability, evolvability and adaptability, constancy and continuity of service, auditing, redundancy, flexibility, compatibility, compliance with the standard.

The extracted criteria, by questionnaire with Lick ret spectrum including odd numbers one till nine inserted. Seven experts were asked about the priorities of these criteria. The scientific experts are staff of Sharif, Amirkabir, Science and technology universities and professional's experts are manager or service provider in cyberspace. Answers of experts, with SPSS program, are evaluated and middle of evaluation is 6.242 and also Cronbach's alpha is 0.893. Twelve criteria are higher than middle, and the other criteria are deleted as shown in Table 1.

In this step for establishing weights of criteria, first we use multiple criteria decision-making analytical hierarchy process (AHP), see Figure 4. For this reason, five experts (two experts are the same as the previous step) answer AHP questionnaire. From the experts' answer, geometric mean was taken. In this state the inconsistency index is 0.07, thus is a satisfactory result. The weight of criteria is Figure 5. The weight of criteria after extracting the weight of criteria, a model will be obtained where input is anything and output is the evaluation of anything in network or graph. If we compare the above result with other methods, then we conclude that the second approach coincides with real work.

3.1.3. Step 3: extracting and analyzing the weights of the criterions and proposing a model

The two criterions of "security" and "privacy" had the highest weights both in geometric and arithmetic averages, indicating their high importance. The criteria of "reputation" and "background" have lower ranks. Namely, a service or a user with a proper reputation and background cannot operate properly in interacting with new services and users and even causes problems in providing new services. Therefore, we should attribute a higher priority to measurable and systematic criterions such as the security, privacy, and stability to assess the trust.

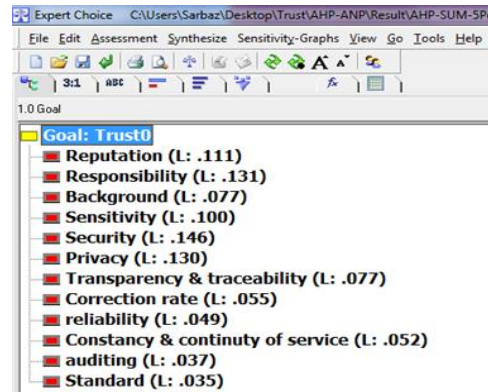


Figure 5. The weight of criteria

3.2. Level 2 (rate of trust in each indicator and formation of the trust graph)

Equations should be placed at the center of the line and provided consecutively with equation numbers in parentheses flushed to the right margin, as in (1). The use of Microsoft equation editor or MathType is preferred. In this study, it is recommended that a complex network, such as a cyberspace network, be converted to a weighted graph whose nodes and weighted edges are the network entities and the degree of trust between the two entities, respectively. To achieve this weighted graph, it is formed with the nodes and edges indicating the entities and the relationship between the entities, respectively. In order to find the trust between the entities, the weight of each index is extracted, and the degree of trust in each index is calculated. In this distributed and graph-based methods proposed to calculate the degree of trust in each indicator, for each indicator, each service must obtain confirmations for that indicator from the trusted entities in the network, so that ultimately, a weight of trust can be calculated for each indicator from among the confirmations provided, see Table 2. Moreover, a method for routing in the graph is presented to find the max reliable trust path for each index, which will be explained in the next sections.

Table 2. Weights of criterions extracted using the ANP method

| ANP Result | Criterion |
|------------|-------------------------------------|
| 0.17535 | Security |
| 0.14097 | Privacy |
| 0.1179 | Constancy and continuity of service |
| 0.09166 | Reliability |
| 0.0871 | Compliance with the standard |
| 0.07934 | Responsible |
| 0.0743 | Transparency and traceability |
| 0.05625 | Correction rate |
| 0.05564 | Auditing |
| 0.04892 | Sensitivity |
| 0.03689 | Background |
| 0.03568 | Reputation |

3.2.1. Step 1: obtaining degree of trust in each criterion

Here, valid and trusted entities in the network are used to obtain trust in each criterion. Trusted entities are professional centers or individuals competent to issue confirmations about the level of trust in the service being investigated. The service examined by the proposed model obtains required confirmations from the trusted entities. Finally, based on the proposed model, the amount of trust in each service is obtained.

3.2.2. Step 2: finding graph-based trust confirmations

For determining the amount of trust in a service, for each of the 12 weighted indexes extracted a graph is formed such that the examined entity as the initial node and the origin of the graph and the desired index is considered as the final node of the graph. Here, the weights of the edges show the view of the intermediate nodes about the amount of the confirmation and trust in that indicator in the desired entity. There may be several paths between the origin and the destination, but there must be at least one path between the origin and the destination containing at least one trusted entity or an intermediate node so that the weight of the desired index can be obtained. A threshold is considered for each indicator, and if the trust

amount in an index is less than this threshold, it will be eliminated from the calculation of the amount of trust in a service; the amount of this threshold depends on the type of use of the model and the service that is examined with this model. Therefore, a path with the least amount of trust should be calculated.

3.2.3. Step 3: max reliable trust path

Since the path with the highest degree of trust for the index to participate in trust calculation is the shortest path, and the routing method is based on finding the best path from the existing paths, then weight of each edge in the graph represents the trust level of the initial node to the end node. So, the path between the origin and destination will have a weight of trust. The variable X in (2) shows that if the path k from node i to node j , to use the edge between them, the value is equal to one or zero [16].

$$\begin{cases} X_{k,i,j} = 1, & \text{if the path } k \text{ uses the line between } i \text{ and } j \\ X_{k,i,j} = 0, & \text{otherwise} \end{cases} \quad (2)$$

Notice that it should be ensured that the path k is got out from the source node, otherwise the program output is invalid. The index $k(1)$ in (3) is the source node number in using routing after the numbering.

$$\forall k: \sum_{j=1}^n X_{k,k(1),j} + \sum_{i=1}^n X_{k,i,k(1)} = 1 \quad (3)$$

The mentioned constraint in (3) also implies that the path should be got out from the node defined as the movement origin and should not be entered again into this node. Similarly, two points should be considered about destination. The sum of movement from neighboring nodes to neighboring nodes should be equal to 1 as showed in (4). The index k in (2) represents the number of destination node [17].

$$\forall k: \sum_{i=1}^n X_{k,i,k(2)} + \sum_{j=1}^n X_{k,k(2),j} = 1 \quad (4)$$

The third constraint is protected the continuity of the path, which means that if a path enters the middle node, it must leave that node [18].

$$\forall k, \forall j: \sum_{i=1}^n X_{k,i,j} = \sum_{i=1}^n X_{k,j,i} \quad (5)$$

The fourth constraint is not redirecting an edge, which means that if a path is entered from one node to another, it will not re-enter from that node to the original node in its path.

$$\forall k, \forall i, \forall j: [X_{k,i,j} + X_{k,j,i}] \leq 1 \quad (6)$$

Finally, the routing selected path lengths between nodes should be minimized. Therefore, the objective function seeks to minimize the path between the source and destination.

3.2.4. Step 4

Now, let us consider a formula for computing a trust for each service same as (1). Therefore, we consider object function for finding a path with at least weight. Let us suppose n nodes of graph and W is $n * n$ matrix then

$$T = \text{Max} \left[\sum_{k=1}^l \prod_{i=1}^n \sum_{j=1}^n X_{k,i,j} * w_{i,j} \right] \quad (7)$$

where, $w_{i,j}$ is an element of matrix including confidence weight for nodes relative to each other. Then,

$$t_{ij} = \sum_k c_{ik} * c_{kj} \quad (8)$$

where t_{ij} is local trust.

Notice that the trust of user searches the value of trust by this process and is called source and goal user is called sink. First, the source searches the value of the sink in neighbors. Neighbors are friends of sink. The above formula is trust of source tends to sink. Notice that j is criterion of sink and k is criterion of source

that has trust to sink. This is only one level of trust of neighbor nodes. This process is followed by all neighbors. For computing trust of two levels of neighbors, one can use (9),

$$t_{il} = \sum_j c_{ij} * c_{jl} + \sum_j c_{ij} \sum_k c_{jk} * c_{kl} \quad (9)$$

where i is source, l is sink, j are neighbors of source and k are neighbors of source and k are neighbors of neighbors of source. This trend will be used till arbitrary depth. It is necessary to say that in the next level the value of trust is less than or equal to the previous level and by normalization the value of trust directly is in intervals $[0, 1]$. By eliminating entities whose trust weight is less than the threshold, a graph with weighted edges called the trust path and the measure is obtained, with the weight of the edges indicating the degree of trust of the entities in each other [19]–[21].

3.3. Data collection

We determined the trust based on graph model. In any social network, it is important for connecting the users. In addition, validation of each service for introducing to government people also is significant. Rankings of the seven social services performed by the organization are evaluated by these formulae.

4. TESTING AND SHOWING RESULTS

Here we test the above formula with scenario attack. Let a bad-mouthing with two states: i) a trust of destructive node in minimum weight on a path; ii) remove the comments of destructive node in computing the maximum value. In this case we have eight paths, one service, three trusted entities and one criterion. So, first the trust for each path is calculated then it is multiplied to the amount of each trusted entity. Then two formulas for computing the trust are applied [22].

By using the formula and in view of (1), (7); $T = \sum_{i=1}^n w_{ik} * v_i \sum_{j=1}^{m_i} t_{ij} * t_{jk}$ namely, trust for each path k and the total trust $T = \text{Max}[\sum_{k=1}^l \prod_{i=1}^n \sum_{j=1}^n X_{k,i,j} * w_{i,j}]$ by taking into account four constraints presented in the previous section is determined.

$$\begin{aligned} \text{For } n_1: i = 1 &\rightarrow \sum X_{1,1,j} * w_{1,j} = 0.4, i = 2 \rightarrow \sum X_{1,2,j} * w_{2,j} = 0.8, \\ i = 3 &\rightarrow \sum X_{1,3,j} * w_{3,j} = 0.7 \Rightarrow T_1 = 0.4 * [0.4 * 0.8 * 0.7] = 0.0896. \end{aligned}$$

$$\begin{aligned} \text{For } n_2: i = 1 &\rightarrow \sum X_{2,1,j} * w_{1,j} = 0.2, i = 5 \rightarrow \sum X_{2,5,j} * w_{5,j} = 1, \\ i = 6 &\rightarrow \sum X_{2,6,j} * w_{6,j} = 0.5 \Rightarrow T_2 = 0.4 * [0.2 * 1 * 0.5] = 0.0040. \end{aligned}$$

$$\begin{aligned} \text{For } n_3: i = 1 &\rightarrow \sum X_{3,1,j} * w_{1,j} = 0.4, i = 7 \rightarrow \sum X_{3,7,j} * w_{7,j} = 0.8, \\ i = 8 &\rightarrow \sum X_{3,8,j} * w_{8,j} = 0.9 \Rightarrow T_2 = 0.4 * [0.4 * 0.8 * 0.9] = 0.1152. \end{aligned}$$

$$\begin{aligned} \text{For } n_4: i = 9 &\rightarrow \sum X_{4,9,j} * w_{9,j} = 0.4, i = 7 \rightarrow \sum X_{4,7,j} * w_{7,j} = 0.8, \\ i = 8 &\rightarrow \sum X_{4,8,j} * w_{8,j} = 0.9 \Rightarrow T_2 = 0.3 * [0.4 * 0.8 * 0.9] = 0.00864. \end{aligned}$$

$$\begin{aligned} \text{For } n_5: i = 9 &\rightarrow \sum X_{5,9,j} * w_{9,j} = 0.3, i = 10 \rightarrow \sum X_{5,10,j} * w_{10,j} = 0.6, \\ i = 3 &\rightarrow \sum X_{5,3,j} * w_{3,j} = 0.7 \Rightarrow T_2 = 0.3 * [0.3 * 0.6 * 0.7] = 0.0378. \end{aligned}$$

$$\begin{aligned} \text{For } n_6: i = 9 &\rightarrow \sum X_{6,9,j} * w_{9,j} = 0.3, i = 11 \rightarrow \sum X_{6,11,j} * w_{11,j} = 0.7, \\ i = 12 &\rightarrow \sum X_{6,12,j} * w_{12,j} = 0.9 \Rightarrow T_2 = 0.3 * [0.3 * 0.7 * 0.9] = 0.0567. \end{aligned}$$

$$\begin{aligned} \text{For } n_7: i = 13 &\rightarrow \sum X_{7,13,j} * w_{13,j} = 0.6, i = 14 \rightarrow \sum X_{7,14,j} * w_{14,j} = 0.9, \\ i = 8 &\rightarrow \sum X_{7,8,j} * w_{8,j} = 0.9 \Rightarrow T_2 = 0.3 * [0.6 * 0.9 * 0.9] = 0.1458. \end{aligned}$$

$$\begin{aligned} \text{For } n_8: i = 13 &\rightarrow \sum X_{8,13,j} * w_{13,j} = 0.9, i = 15 \rightarrow \sum X_{8,15,j} * w_{15,j} = 1, \\ i = 8 &\rightarrow \sum X_{8,8,j} * w_{8,j} = 0.9 \Rightarrow T_2 = 0.3 * [0.9 * 1 * 0.9] = 0.243. \end{aligned}$$

Thus, $T = \max_i T_i = 0.243$.

If threshold (the condition to employ each path) be, for instance, $\min(\text{validations}) \geq 0.05$, the above values are acceptable. So, $\max(\min(\text{validations of nodes in path})) = 0.4$ is the trust of criterion by trusted unity 1, such that $\min(\text{validations of nodes in path}) \geq 0.05$, and so on. Then, the total trust coincides with (9) is,

$$T = \max [0.4 * 0.4, 0.4 * 0.2, 0.4 * 0.4, 0.3 * 0.4, 0.3 * 0.3, 0.3 * 0.3, 0.3 * 0.6, 0.3 * 0.9]$$

$$\Rightarrow T = \max[0.16, 0.8, 0.16, 0.12, 0.9, 0.9, 0.18, 0.27] = 0.27.$$

Therefore, the result of the second formula is better than the first.

5. DISCUSSION AND IMPLICATION

5.1. Discussion of findings for case study

Since trust has a social aspect, in step 5, to examine a case and to test the proposed trust model, seven social messaging cyberspace services, as public and widely used social services, were evaluated and ranked. The services considered have been evaluated by a reliable organization. In this article, the services were evaluated with the criterion and the proposed model more accurately with more details, and better results were obtained as compared to the evaluation carried out by that organization [23].

Three main factors have been considered in evaluation and ranking conducted by the organization: i) planning that shows designs and technologies used in each service (say, *P* in (9)); ii) security (*S*) and the usage (*E*) that represents the adoption of the service by users. The three evaluation factors have been selected based on the opinions of organizational and academic experts. To reach a certain degree of trust for each service, each of the three factors have been weighted based on the experts' opinions according to (8).

$$T = 0.4 * P + 0.3 * S + 0.3 * E \tag{10}$$

Here, to perform the evaluation with more detail and accuracy, the effect of each of the 12 extracted criterions in Table 1 on each of the three factors mentioned in (7) in each of the seven considered services was examined, and one table was obtained for each of the three factors in (10). As shown in Figure 6, there are three main factors at the first level and 12 trust criterions at the second level shown by *Fi*. The evaluation was carried out by 3 experts. Finally, after calculating the average of the experts' opinions and according to (10), these three tables were merged and according to Table 2, the degree of trust to each of these seven services was obtained [24].

Finally, in order to evaluate the accuracy of the proposed model and the results, the degree of trust obtained from this study was compared with the level of users trust for each service, as shown in Figure 7. The level of user trust that results from the level of user application and satisfaction with these services is obtained by 3 indicators of the number of registered users, the number of active users, and the traffic volume of each service. The correlation coefficient Pierson is 70.37%, indicating appropriate trust results extracted from this model [25].

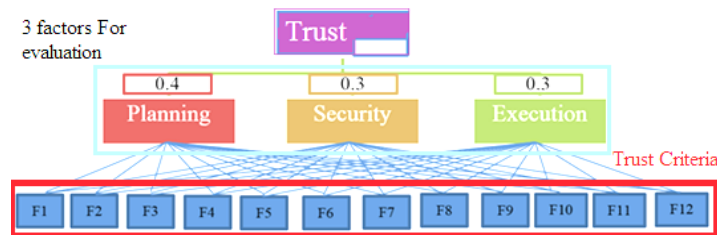


Figure 6. Examining the effect of the 12 criterions on the three main factors

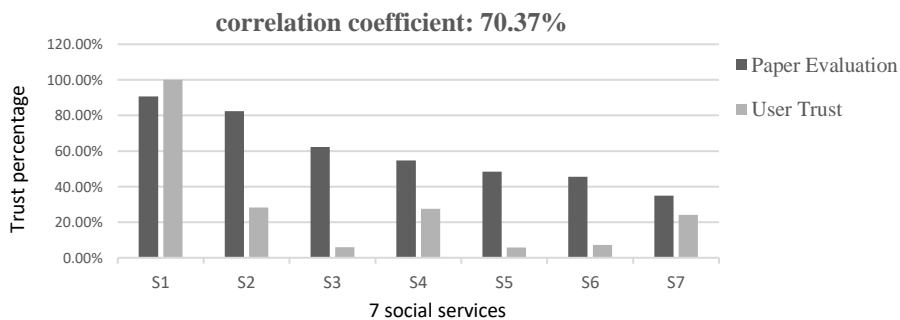


Figure 7. Rankings of the seven social services performed by the organization and by the article

One of the most important reasons for the slight difference between the two evaluations is that the evaluation carried out in this paper with 12 technical criteria and by considering their effect on the three factors of design, security, and usage, without considering social and usage criteria. However, in the evaluation performed by the organization, the usage criterion has been independent and important. Although the usage factor has been considered by ours, the factor is not independent, and since we have taken into account the effect of the 12 technical criteria on the three factors, our results would be technical, not social. In other words, the usage factor has been taken into account in our study from the perspective of the 12 technical criteria. That is why service S3, due to its poor design, has obtained a lower rank based on our evaluation, but it has obtained a higher rank in the evaluation performed by the organization due to its better position resulting from its adoption by users. Trust percentage 7 social services.

5.2. Limitations and future research directions

Despite the significant findings of this study, our results should be interpreted in the networks. This study identified the criteria of trust based on service and content provision. Future studies should explore various factors that may affect the development of trust models. Since there were some limitations including the limited time and consequently the limited use of experts, using other multi-criteria decision-making models, including fuzzy models, was not possible. We suggest that in future research, fuzzy models will be used to increase the accuracy, interpretive structural modelling (ISM) methods will be used to establish level of criteria, and the decision-making trial and evaluation laboratory (DEMATEL) method will be used to determine the criteria that are effected or affected.

6. CONCLUSION

In this paper, the goal is computation a trust of things. In order to find a role, the criteria of this field were extracted. Then the experts characterized the priorities of criteria. Computation of answers shows that the criteria is satisfactory. Then from 26 criteria twelve criteria are selected. Thus, the experts characterized the weights of each criterion. Then, the trust criteria were weighted using the ANP and AHP methods. Based on real world we focus on ANP results, and the two criteria of “security” and “privacy” had the highest weights, and the relationships between the criteria were determined. The model can be used to extract a trust weight for every cyberspace entity including its services and users, and one can decide which services can be trusted in terms of the importance and the sensitivity of the model user. Using the extracted weights, one graph was proposed for each criterion where each user or service can reach the lowest trust weight by passing through the path with the lowest trust weight, and finally, a weighted graph with the lowest degree of trust of entities to each other was proposed. Furthermore, to test the model, due to the importance of the sociality of trust, seven public and widely used cyberspace social services were weighted using the model, and because a proper correlation coefficient was obtained, our results comparing to the evaluation by the organization are acceptable.




REFERENCES

- [1] N. A. Mhetre, A. V. Deshpande, and P. N. Mahalle, “Trust management model based on fuzzy approach for ubiquitous computing,” *International Journal of Ambient Computing and Intelligence*, vol. 7, no. 2, pp. 33–46, Jul. 2016, doi: 10.4018/IJACI.2016070102.
- [2] M. Al-Ississ and I. Bohnet, “Risk mitigation and trust: experimental evidence from Jordan and the United States,” *Journal of Economic Psychology*, vol. 53, pp. 83–98, Apr. 2016, doi: 10.1016/j.joep.2015.12.010.
- [3] D. Artz and Y. Gil, “A survey of trust in computer science and the semantic web,” *Journal of Web Semantics*, vol. 5, no. 2, pp. 58–71, Jun. 2007, doi: 10.1016/j.websem.2007.03.002.
- [4] S. Bhattacharya, D. Wainwright, and J. Whalley, “Internet of things (IoT) enabled assistive care services: Designing for value and trust,” *Procedia Computer Science*, vol. 113, pp. 659–664, 2017, doi: 10.1016/j.procs.2017.08.333.
- [5] G. Büyüközkan, S. Gülleryüz, and B. Karpak, “A new combined IF-DEMATEL and IF-ANP approach for CRM partner evaluation,” *International Journal of Production Economics*, vol. 191, pp. 194–206, Sep. 2017, doi: 10.1016/j.ijpe.2017.05.012.
- [6] I.-R. Chen, J. Guo, and F. Bao, “Trust management for SOA-based IoT and its application to service composition,” *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482–495, May 2016, doi: 10.1109/TSC.2014.2365797.
- [7] J.-H. Cho, K. Chan, and S. Adali, “A survey on trust modeling,” *ACM Computing Surveys*, vol. 48, no. 2, pp. 1–40, Nov. 2015, doi: 10.1145/2815595.
- [8] C. Chou, “Application of ANP to the selection of shipping registry: The case of Taiwanese maritime industry,” *International Journal of Industrial Ergonomics*, vol. 67, pp. 89–97, Sep. 2018, doi: 10.1016/j.ergon.2018.04.009.
- [9] I. Ud Din, M. Guizani, B.-S. Kim, S. Hassan, and M. Khurram Khan, “Trust management techniques for the internet of things: a survey,” *IEEE Access*, vol. 7, pp. 29763–29787, 2019, doi: 10.1109/ACCESS.2018.2880838.
- [10] G. D. Tormo, F. G. Mármol, and G. M. Pérez, “Dynamic and flexible selection of a reputation mechanism for heterogeneous environments,” *Future Generation Computer Systems*, vol. 49, pp. 113–124, Aug. 2015, doi: 10.1016/j.future.2014.06.006.
- [11] J. Guo, I.-R. Chen, and J. J. P. Tsai, “A survey of trust computation models for service management in internet of things systems,” *Computer Communications*, vol. 97, pp. 1–14, Jan. 2017, doi: 10.1016/j.comcom.2016.10.012.




- [12] C.-W. Hang and M. P. Singh, "Trustworthy service selection and composition," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 6, no. 1, pp. 1–17, Feb. 2011, doi: 10.1145/1921641.1921646.
- [13] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks," *ACM Computing Surveys*, vol. 49, no. 1, pp. 1–35, Jul. 2016, doi: 10.1145/2906151.
- [14] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, Mar. 2007, doi: 10.1016/j.dss.2005.05.019.
- [15] M. Kara, "Review on common criteria as a secure software development model," *International Journal of Computer Science and Information Technology*, vol. 4, no. 2, pp. 83–94, Apr. 2012, doi: 10.5121/ijcsit.2012.4207.
- [16] R. Kiani Mavi and C. Standing, "Critical success factors of sustainable project management in construction: A fuzzy DEMATEL-ANP approach," *Journal of Cleaner Production*, vol. 194, pp. 751–765, Sep. 2018, doi: 10.1016/j.jclepro.2018.05.120.
- [17] R. Kumar, S. A. Khan, and R. A. Khan, "Analytical network process for software security: a design perspective," *CSI Transactions on ICT*, vol. 4, no. 2–4, pp. 255–258, Dec. 2016, doi: 10.1007/s40012-016-0123-y.
- [18] P. Martinez-Julia and A. F. Skarmeta, "Beyond the separation of identifier and locator: Building an identity-based overlay network architecture for the Future Internet," *Computer Networks*, vol. 57, no. 10, pp. 2280–2300, Jul. 2013, doi: 10.1016/j.comnet.2012.11.020.
- [19] D. Ott, C. Vishik, D. Grawrock, and A. Rajan, "Trust evidence for IoT: trust establishment from servers to sensors," in *ISSE 2015*, Springer, 2015, pp. 121–131.
- [20] A. Razaque, F. Amsaad, S. Hariri, M. Almasri, S. S. Rizvi, and M. B. H. Frej, "Enhanced grey risk assessment model for support of cloud service provider," *IEEE Access*, vol. 8, pp. 80812–80826, 2020, doi: 10.1109/ACCESS.2020.2987735.
- [21] S. K. Madria, "Security and risk assessment in the cloud," *Computer*, vol. 49, no. 9, pp. 110–113, Sep. 2016, doi: 10.1109/MC.2016.280.
- [22] K. Djemame, D. Armstrong, M. Kiran, and M. Jiang, "A risk assessment framework and software toolkit for cloud service ecosystems," *Cloud computing*, vol. 5, pp. 119–126, 2011.
- [23] Z. Zhang and A. Meddahi, *Security in network functions virtualization*. Elsevier, 2017.
- [24] J. Moura and D. Hutchison, "Review and analysis of networking challenges in cloud computing," *Journal of Network and Computer Applications*, vol. 60, pp. 113–129, Jan. 2016, doi: 10.1016/j.jnca.2015.11.015.
- [25] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, Mar. 2012, doi: 10.1016/j.future.2010.12.006.

BIOGRAPHIES OF AUTHORS






Mostafa Heidarzadeh Kalahroudy    received the B.Eng. degree in Computer Engineering from Shahed University 2005 and the M.S. from Amirkabir and Ph.D. degrees in Software Engineering from Ghom University, in 2010, 2021, respectively. His research interests include artificial intelligence applied in pure mathematics and modelling systems. He can be contacted at heydarzadeh.mostafa@yahoo.com.



Kheirollah Rahsepar Fard    is faculty staff of Technological and Engineering of Ghom University. He received a Ph.D. in Applied Mathematics in 2011. His research interests are financial mathematics, multivariate polynomial interpolation, numerical analysis, and numerical solution of linear algebra. He can be contacted at rahsepar@qom.ac.ir.



Yaghoob Farjami    is at Department of Computer and Information Technology at Ghom University. His research interests are numerical analysis and numerical solution of linear algebra. He can be contacted at farjami@gmail.com.