

# We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,100

Open access books available

149,000

International authors and editors

185M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index  
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?  
Contact [book.department@intechopen.com](mailto:book.department@intechopen.com)

Numbers displayed above are based on latest data collected.  
For more information visit [www.intechopen.com](http://www.intechopen.com)



# Trust Management: A Cooperative Approach Using Game Theory

*Ujwala Ravale, Anita Patil and Gautam M. Borkar*

## Abstract

Trust, defined as the willingness to accept risk and vulnerability based upon positive expectations of the intentions or behaviours of another. The qualities or behaviours of one person that create good expectations in another are referred to as trustworthiness. Because of its perceived link to cooperative behaviour, many social scientists regard trust as the backbone of effective social structures. With the advancement in technology, through these online social media people can explore various products, services and facilities. Through these networks the end users want to communicate are usually physically unknown with each other, the evaluation of their trustworthiness is mandatory. Mathematical methods and computational procedures do not easily define trust. Psychological and sociological factors can influence trust. End users are vulnerable to a variety of risks. The need to define trust is expanding as businesses try to establish effective marketing strategies through their social media activities, and as a result, they must obtain consumer trust. Game theory is a theoretical framework for analysing strategic interactions between two or more individuals, in the terminology of game theory, called players. Thus, a conceptual framework for trust evaluation can be designed using a game theory approach that can indicate the conditions under which trustworthy behaviour can be determined.

**Keywords:** trust, cooperative behaviour, game theory, sociological factors, vulnerable

## 1. Introduction

Trust is a subjective, multi-faceted, and abstract notion. In addition to computer technology, many researchers worked on trust for a variety of fields, including business, philosophy, and social science. Analysts from diverse domains concur with the basic definition of trust, i.e., it is measurement of the trustworthiness of a person or any living things. Trust is regularly inferred from certain input appraisals through aggregation of trust.

Trust has been classified as a black-box, or undifferentiated variable, in the massive number of studies, and has rarely been investigated in depth. Even if it appears in predictable ways, trust is not a one-dimensional or homogeneous idea. Trust is viewed as a multi-faceted notion that can be interpreted differently depending on the context. In addition to computer technology, trust has been

studied in a variety of fields, including economics, psychology, and social studies. Researchers from several fields agree on the basic definition of trust, that is trust characterises an individual's level of anticipation and trustworthiness, also shows cooperative relation between inter organisational entities. Trust is derived from specific feedback evaluation and mechanism. It has been discovered that trust reduces disagreement and uncertainty by fostering goodwill that strengthens relationships while also increasing satisfaction and partners' willingness to trade.

Trust management encompasses trust as an identification and communication establishment of the elements with different techniques for computation, transmission, consolidation, and information storage, consumption models and enhancement in service provisioning of trust. Certain trust functionality can be implemented and supported using distributed computing. Decentralised trust management refers to the administration of trust in fully decentralised computer systems as well as hybrid centralised-decentralised computing systems.

Trust management has infiltrated a wide range of collaborative networked computing systems, including peer-to-peer and eCommerce, social networks and online communities, cloud and edge computing, mobile ad hoc networks and wireless sensor networks, community sourcing, multi-agent systems, and the Internet of things [1].

### **1.1 Different trust management models**

- **Community trust:** community trust is a term that refers to the trust that people have for one another. In the context of decentralised network and application, trust management in one-to-one systems. Low incentive systems for providing ratings, bias toward positive feedback, unauthenticated participants, fake or illegal feedback rating from malicious individuals, altering authentications, etc. are some of the primary difficulties in developing and using trust.
- **Multi-agent trust:** trust is defined to promote collaboration/cooperativeness among several independent entities in order to complete a task. The autonomy, inferential capability, responsiveness, and social behaviour of an agent were characterised by Balaji and Srinivasan [2]. Granatyr et al. [3] examined multi-agent system trust models by examining a number of trust terminologies: semantics, preference, delegation, risk measure, incentive, feedback, open environment, hard security threats, and requirements. These all terminologies are with types of interaction such as alliance, logical reasoning, compromise, and prerequisite. Pinyol et al. [4] evaluated trust in cognition, method, and generality in Pinyol and Sabater-Mir [4]. From a game theoretic standpoint, trust features are evaluated as a use of numerous input sources, the use of cheating assumptions, and the providing of procedural and intellectual ideas.
- **Social networks:** Sherchan et al. [5] looked at reactive, non-transferable features, interaction behaviours, and past experiences as well as other important aspects of social trust. Jiang et al. [6] classified graph-based theory uses to define evaluation approaches for online social networks into two categories: graph simplification-based and analogy-based approaches.
- **Trust in wireless ad-hoc network:** in mobile and wireless sensor networks, trust is a prominent approach use to secure routing with QoS [7]. In WAN, trust metrics into the routing protocols provides decision making, correctness, optimal path finding. A number of trust frameworks for dealing with the bad-mouthing and double-face attacks. Loop attacks, worm-hole, blackhole, grey

hole, DoS, data modification/insertion attacks, sinkhole, contradictory behaviour attacks, and so on are examples of potential assaults.

- **Trust in cloud computing:** in cloud computing, trust management defines the following types: (i) policies or rules; (ii) recommendations; (iii) reputations; and (iv) predictions. Ahmed et al. [8] proposed a survey to evaluate trust as a link between customer and service provider. It was stated that the general requirements for trust evaluation consist of general guidelines and cooperative behaviour of the stakeholders.
- **Trust in cryptography:** Kerrache et al. [9] analyse an existential threat on trustworthiness and cryptography for mobile adhoc networks. The reply attack, masquerading attack, privacy assault, security communication attacks, DoS attacks, etc. are considered to define the need for a trust mechanism for application safety. In addition to standard attacks like masquerade and impersonation, Sybil attack, and location trapping, the infotainment application largely featured retransmission message assault and illusion attack.
- **Trust in multi-disciplinary research:** from a multidisciplinary standpoint, trust has been a recurring subject. Cho et al. [10] analysed the hybrid trust by computing various parameters such as communication, data exchange, cooperative work, etc. and covered different domains like artificial intelligence, human machine interaction, database, machine learning, computer networks, information security, etc.

## 2. Related study

All of our social interactions are built on the foundation of trust. Trust is a complex human habit that has evolved over time. Trust has many various interpretations, and as a result, many alternative representations and management principles, depending on the circumstances and applications. It has been a research issue in many domains, including psychology, sociology, IT systems, and so on. For example, trust is utilised in trade systems like eBay and automatic Peer-to-Peer systems like file and resource sharing, where trust is built by algorithms based on prior events, which provide either good or negative evidence or feedback.

In online systems, there are two sorts of trust: direct trust, which is based on a person's direct connection with others, and recommendation trust, which is based on the experiences of other individuals in a social network and grows in a sense based on the propagative feature of trust. Different trust management models are discussed in below section.

Wang et al. [11] developed a game theory-based trust evaluation model for social networks. As a result, when modelling a trust relationship, various factors must be taken into account. The trust value is calculated by considering three factors mainly: feedback efficacy, service reliability and suggestion credibility. In social networks, service transactions are based on node-to-node trust links. Building a trust relationship, on the other hand, is a long and winding process impacted by previous contacts, trust recommendations, and trust management, among other things.

Jian et al. [12] proposed a trust model basically for online social networks using evidence theory techniques. Evidence theory is mostly used for target identification, decision making and to analyse online social networks. The proposed model mainly contains three steps i.e. to achieve individual trust evaluation, determine the relevance of features with respect to each user, which is used for decision making.

Trust evidence approach is to show the probability of trust and distrust among the stakeholder. This approach achieves an error rate which is minimal and highest accuracy in the dataset Epinions.

Chen et al. [13] provided a trust evaluation model using a machine learning algorithm that takes into account a wide range of trust-related user attributes and criteria to enhance human decision-making. User features are classified into four categories based on the empirical analysis: link-based features, profile-based features, feedback-based features, behaviour-based features. Then a lightweight attribute selection technique based on users' online information to analyse the efficiency of each feature and identify the ideal combination of features using users' online information in the form of records. Results are conducted on real-world dataset to show the overall performance which is better as compared to other traditional approaches.

In the current era, Online Social networks have an essential role in practically every aspect of life, and their presence can be seen in all aspects of daily life. Metaheuristic search algorithms are used in social networks due to the property of dynamic nature which it exhibits.

Peng et al. [14] proposed a feature fusion technique in conjunction with an artificial bee colony (ABC) for community identification task to improve performance in terms of accuracy in trust-based community detection using an artificial bee colony (TCDABCF). This strategy takes into account not only an individual's social qualities, as well as in a community the relationship of trust that exists between users is also considered. As a result, the proposed technique may result in the finding of more appropriate clusters of similar users, each with significant individuals at the centre. Proposed technique makes use of an artificial bee colony (ABC) to accurately identify influential persons and their supporters. For simulation purposes, the Facebook dataset is used and the proposed method has obtained 0.9662 and 0.9533 Normalised mutual Information (NMI) and accuracy, respectively.

Reputation and trust prediction are "soft security" solutions that allow the user to evaluate another user without knowing their identity. The trustworthiness of users in social networks is calculated using the reputation level of other users. A new probabilistic reputation feature is more efficient than raw reputation features. Various machine learning algorithms and 10-fold cross validation proposed by Liu et al. [15] is used for simulation. The witness trustor users' trust values are used to determine the trustee's reputation qualities. Raw and probabilistic reputation features, which are two different types of characteristics, were compared. Three datasets namely wiki, Epinions and Slashdot are used for simulation purposes. SMOTE boost algorithm is used to balance the dataset to improve prediction performance of prediction. In online social networks, this trust prediction algorithm can be used to strengthen social relationships and identify trustworthy users.

The recommended approach proposed by Mohammadi et al. [16] took into account users' attitudes toward one another on a social network as the basis of their trust. The mostly textual contents shared on social networks were analysed to determine how people felt about one another. In this Sense trust model, initially analysis of hidden sentiments between the texts exchanged between two social network users are taken into consideration. Then Hidden Markova Model is used to evaluate trust between users on social networks. Statements exchanged; Hidden Markov Model (HMM) is utilised. Both RNTN and HMM are trained with emails extracted from Enron Corporation undergoing crowdsourcing and labelling.

A trust framework by Hansi et al. [17] introduced the proposed methodology to determine the node trust values for social network users using reinforcement

Study	Technique	Parameters used	Limitations/future work
Wang et al. [11]	Game theory approach	Service reliability, feedback effectiveness, and recommendation credibility. Resolves free riding problem	More specific trust relationships between nodes, for example, family, best friends, and classmates.
Jiang et al. [6]	Using evidence theory	Weight set is the importance degree of each user features and scope set is a set of value range to generate trust evidence	Weight determination can be implemented for trust evidence.
Chen et al. [13]	Lightweight feature selection approach using machine learning	User features are divided as profile-based features, behaviour-based features, feedback-based features, and link-based features.	To analyse the temporal features of trust to build a dynamic trust framework
Peng et al. [14]	Artificial bee colony by feature fusion	Social Features of users, but also their relationship of trust between users in a community	Multi-objective artificial bee colony algorithms can be proposed.
Mohammadi et al. [16]	Hidden Markova Model (HMM)	Statements exchanged among users & level of sentiments in statements are identified.	Other interactions by users like audio, video sharing and other interactions such as like and dislike can be considered.
Hansi et al. [17]	Trust Evaluation using Reinforcement Learning	set of neighbour nodes, Similarity and difference between neighbour nodes	Prevention of information from an untrusted user will make the social network secure and private.

**Table 1.**  
*Comparison of trust management methods.*

learning. On social media trust between two nodes is evaluated based on the features i.e. number of neighbour nodes, relationship among the nodes and number of common neighbour nodes. After selecting features if there is a edge among two nodes, the trust value is denoted as 1 otherwise 0. Second, the node trust will be determined using a training model value. After that, a recommendation algorithm will be used to determine the results. Finally, the simulation is used to analyse the effectiveness of the suggested strategy For the purpose of simulation data from an adaptable social network will be used.

To address the trust evaluation problem in trust social networks, Liu et al. [18] presented NeuralWalk, a machine learning-based approach. Unlike traditional methods, NeuralWalk models singlehop trust propagation and trust combining using a neural network architecture called WalkNet. When the NeuralWalk method is used, WalkNet is trained. Advogato dataset is used to evaluate the accuracy of algorithm. TheNeuralWalk algorithm, in collaboration with WalkNet, does a BFS multi-hop trust assessment across TSNs (**Table 1**).

### 3. Trust-building mechanisms

- Mutual trust
- Proven experience and reputations
- Awareness of the hazards associated with opportunistic behaviours

Web applications	Stakeholder	Trust mechanism scheme
Facebook	End user	User profiles with social networking services
Linked In	End user, different Organisations	User profiles with social networking services
e-commerce web sites (e.g. Flipkart)	Consumer and business	Feedback mechanism
eTransport (e.g. Uber)	Driver and passenger	Rating and driver performance
OYO	Restaurant holder and customer	Customer rating and service review comments

**Table 2.**  
*Trust mechanisms in online social networks.*

- Legal agreement
- Changing processes

An online platform’s trust mechanism is a method for overcoming knowledge gaps between market players and facilitating transactions. Many different types of trust mechanisms exist that are listed below (**Table 2**):

To develop trust among users in a social network is critical. It is critical to study in depth all possible ties between users in the social network and to appropriately evaluate those relations in order to determine who-trusts-whom and integrate that knowledge in the social recommender.

To estimate trust some models use a behavioural pattern of user interaction. Few parameters which are consider to calculate trust are as follows:

- i. Measures such as number/sequence of reviews, number/sequence of rates, and average of number/length of comments posted, among others, are used to categorise user actions in terms of information shared such as reviews, comments posted, ratings, and so on.
- ii. Categorising binary interactions for interactions/relations between two individuals, such as author and rater, author and author, and rater and rater.
- iii. Interactions or flows between users.
- iv. The type of flow between agents or the nature of interactions (for example intimate or not).
- v. The neighbourhood structure of the nodes (for example many mutual friends) etc.

#### 4. Techniques for trust evaluation

Different trust evaluation techniques are classified as Statistical and machine learning approaches, heuristics-based techniques, and behaviour-based techniques. Statistical and machine learning techniques aim to provide a mathematical model for trust management that is sound.

The goal of heuristic-based strategies is to define a feasible model for constructing reliable trust systems. User behaviour in the community is the focus of behaviour-based models.

## 5. Trust evaluation methods

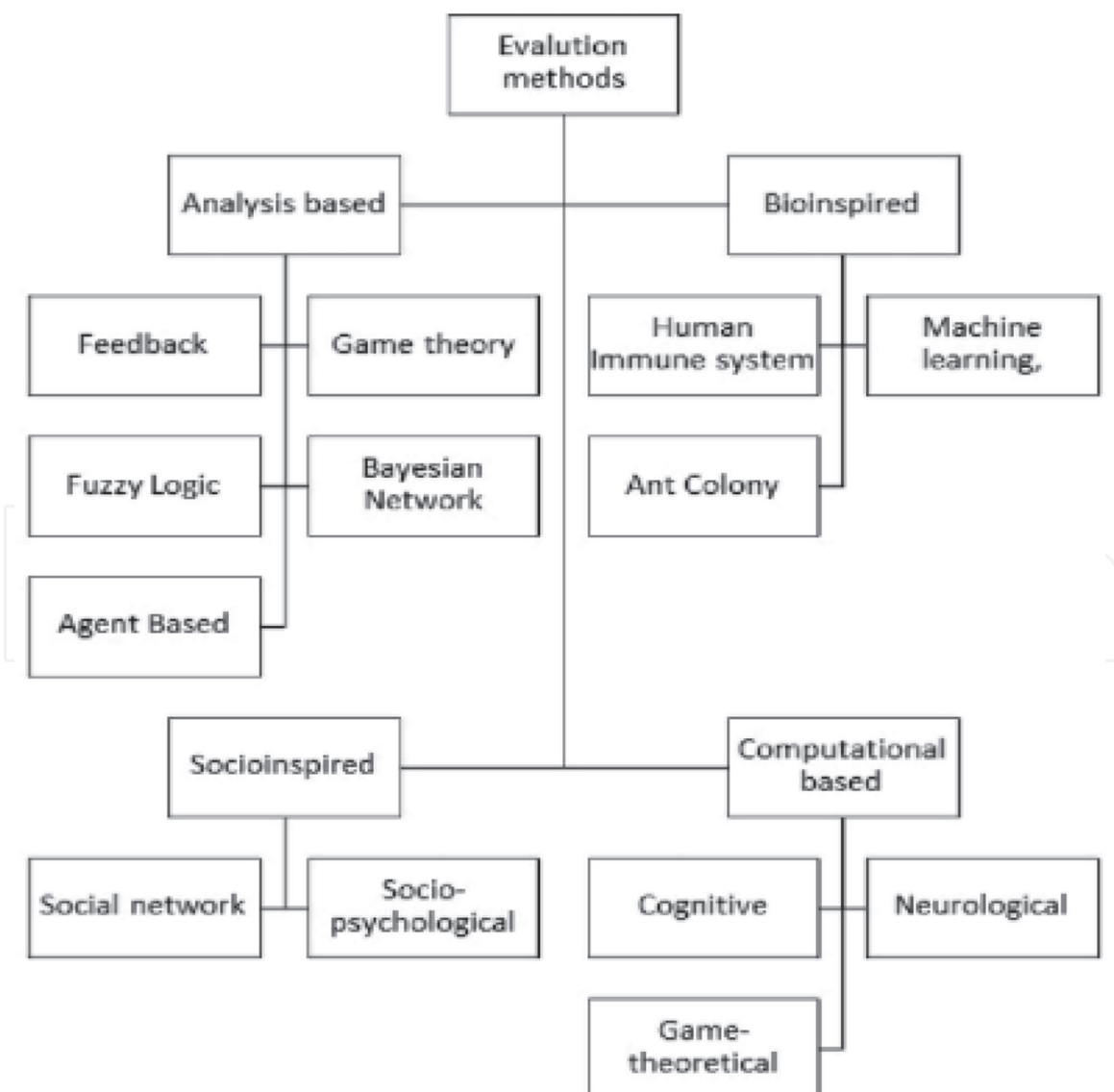
See **Figure 1**.

### 5.1 Analysis of trust evaluation methods

The practise of assessing trust using attributes that influence trust is known as trust evaluation. It is confronted with a number of serious challenges, including a shortage of critical assessment data, a requirement for data processing, and a request for a straightforward participant statement to decision making. Analysis of trust is achieved by using following methods:

#### 5.1.1 Fuzzy logic approach

Trust evaluation model using fuzzy logic in various IOT applications considers the parameters like device physical security, device security level and device ownership trust [19]. Cloud computing plays a very important role on the internet to provide various useful services. In cloud environments trustworthiness of nodes is determined by performance in terms of response time and workload is considered.



**Figure 1.**  
*Different trust evaluation methods.*



Another parameter which is used is known as elasticity in terms of scalability, security, usability and availability [20]. In Wireless Sensor Network fuzzy based trust prediction model trust is calculated in intra cluster and inter cluster level. Trust computation is performed using direct trust and indirect trust interaction among the nodes [21].

### *5.1.2 Game theory approach*

In Online social network trust degree is calculated using three parameters like feedback effectiveness, service reliability and recommendation credibility. In wireless sensor network game theory approach is used to mitigate security attacks. In WSN it mainly calculates parameters like cooperation, reputation and security level from the information collected from the network. In a cloud computing environment trust is evaluated for both user and server providers.

### *5.1.3 Bayesian network*

Users in a virtual world, such as an e-commerce marketplace, are unable to physically inspect the quality of trade products before purchasing them, nor can they secure the security of personal data, resulting in uncertainty and mistrust among network actors. In wireless sensor networks direct trust values are calculated using Bayesian theory and when there is uncertainty in direct trust, indirect trust values are calculated using entropy concept.

### *5.1.4 Feedback approach*

Trustworthiness is achieved by participants' behaviour and feedback. In the network many Quality-of-Service parameters are considered for evaluating behavioural trust value. In Cloud computing, service level agreement parameters are assumed to maintain the feedback and compute the feedback trust value of the cloud service provider [22]. Feedback proves the genuineness of participants.

### *5.1.5 Agent based Approach*

In wireless sensor networks, mobile nodes are used as a router to transfer packet and communication established between nodes. So, every node or agent that is required to be trusted to each other [23]. If a malicious node enters the communication channel, then the network will disturb. So, trust model gives proper security and provides support for decision making.

## **5.2 Bio-inspired trust and reputation model**

A trust model and reputation model mainly consist of components like collecting information, performing ranking, entity selection, transaction and finally reward points. To select the most trustworthy node, it is based on a bio-inspired ant colony algorithm. To select the most trustworthy node, comparison of average phenomenon is done with predefined threshold value, if it is larger than node is trustworthy.

Machine Learning based Trust Evaluation Model: Trust evaluation model based on machine learning can overcome the problems like cold start and zero knowledge which is a disadvantage of traditional trust evaluation models. Machine learning algorithms like logistic regression, K Means, DBscan, SVM, Artificial Neural Network and Decision Tree algorithms are used to determine direct trust value based on trust related attributes.

Ant Colony optimization for Trust Evaluation: Ant Colony Optimization (ACO) is a metaheuristic approach which is used to solve problems of existing models. In wireless sensor networks ACO finds shortest path for packet transmission in a network and accordingly updating of trust value is performed. In online social networks trust value is calculated by activities performed between users.

Human Immune System: Artificial immune system is inspired from Human immune system to provide solution against security attacks in IoT, Wireless sensor network. Which builds the secure environment among the sensor network and evaluates trust between nodes. Different security algorithms and techniques are evaluated based on the immune system such as the IDS system.

### **5.3 Socio-inspired method**

The socio-inspired class of methods draws its inspiration from human psychology shown during historical and psychological relationships. Mankind has natural and inherent competitive inclinations, as well as the ability to collaborate, work together, and interact socially and culturally. This natural behaviour is used to build trust among them. All of these natural behaviours assist an individual in learning and imitating the actions of other humans, allowing them to adapt and enhance their own behaviours throughout time [24]. Individuals tend to adapt and evolve faster through interactions in their social setup than through biological evolution based on inheritance, which gives rise to this family of trust evaluation methods.

Social network: Social networks have grown in popularity as a means of sharing information and connecting people with similar interests. Enterprises and governments stand to benefit greatly from the public accessibility of such networks, as well as the capacity to share opinions, thoughts, information, and experience [5]. Social trust defines with three parameter such as trusted information gathering, evaluation of trust value, and trust dissemination. In social networks, trust evaluation model categories as sociological trust like emotions, behavioural activities of users and computational trust evaluated from sociological trust value.

Socio-physiological: Because the media has such a large influence on public consciousness in today's environment, the question of trust is important. People create firm opinions on many issues based on what they have heard in the news or read on the Internet [25]. As a result, a person gets exposed to several aspects of media such as television, newspapers, and broadcast media at the same time. Most people believe that the information they receive is the only one that is right, which leads to the establishment of false beliefs that have nothing to do with the truth.

### **5.4 Computational methods**

Trust is an important entity for successful finance and social networks. If trust factor is disabled then the entire system will collapse so mathematical modelling is built to define trust value in such applications [26]. Computational trust is measured using game theory approach, cognitive approach and neurological approach.

## **6. Game theory approach for social media**

Game theory approach used in different fields for decision making such as cloud computing, mobile adhoc network, etc. In cloud computing, Nash equilibrium (NE) enhances the trust evaluation at boot load level for service provider and end user or participant [27]. It also prohibits service provider and customer to breach service level agreement. The mathematical study of cooperation and conflict is known as

game theory. It offers a unique and interdisciplinary approach to the study of human behaviour that may be used to any circumstance in which each player's choice effects the utility of other participants, and in which players take this mutual influence into account while making decisions. This type of strategic interaction is often utilised in the study of human-centered systems, such as economics, sociology, politics, and anthropology. Game theory is a powerful conceptual and procedural tool for studying social interaction, including game rules, informational structure of interactions, and payoffs associated with certain user decisions. Game theory may be used to all behavioural fields in a unified approach. Game theory is a powerful conceptual and procedural tool for studying social interaction, including game rules, informational structure, and payoffs associated with specific user decisions.

A game will be defined in the framework of Game Theory as a conflict between two agents: G—a trustworthy agent that receives data, and U—an agent that transmits data. There are two strategies available to players. For agent G, there are two options: trust the agent U or do not trust the agent U. For agent U, the first approach is to send proper data, whereas the second strategy is to send false data. Payments when players win/lose can be designed in order to consider the game in its usual form and express it through the payment matrix.

Because agent G cannot check or dispute the data at the time of receipt, the danger of losing reliable data must be considered. This involves the introduction of the concept of data value. Consider INFO<sub>i</sub> belongs pre-exist information in the system. so  $\exists v(\text{INFO}_i): v(\text{INFO}_i) \neq v(\text{INFO}_j), i \neq j$  is means maximum information i is transmitted. Assume that value of data or information decreases with time. So  $\exists t_f: 0 < t_f \leq t$  is receiving information at time t, then  $\exists v(\text{INFO}_i, t_f, t): v(\text{INFO}_i, t_f, t) \leq v(\text{INFO}_i)$  is the value of the data i at the time t. It can be calculated by the equation:

$$v(\text{INFO}_i, t_f, t) = v(\text{INFO}_i) \times k_{\text{INFO}_i}(t_f, t), \quad (1)$$

where  $k_{\text{INFO}_i}(t_f, t)$  is the function of relevance of the information i at time t. We consider  $k(t_f, t) \neq 0$  as long as the agent cannot disapprove the information, so, let an exponential function of the form  $E_x$  represented in equation to calculate actual data on social network:

$$k_{\text{INFO}_i}(t_f, t) = (E_x \text{ INFO}_i)^{t - t_f} \quad (2)$$

Payoff function (G) of the agent is presented as can be described by the equation

$$f_G(x, y) = \begin{cases} v(\text{INFO}_i) & x = 1, y = 1 \\ 0 & x = 1, y = 2 \\ v(\text{INFO}_i, t_f, t) & x = 2, y = 1 \\ v(\text{INFO}_i, t_f, t) & x = 2, y = 2 \end{cases} \quad (3)$$

where x, y is the number strategies of the agent G and U. For the agent U, the biggest gain will be the value  $\text{Truth}(\text{INFO}_i) = 1$  of the agent G, in the case when the agent U lied, and minimal - when the agent G has trust to U, and U provided him with correct data. To denote the wins of the agent U, we introduce the payoff function, presented in following equation.

$$f_U(x, y) = \begin{cases} -1, & x = 1, y = 1 \\ 1, & x = 1, y = 2 \\ 0, & x = 2, y = 1 \\ 0, & x = 2, y = 2. \end{cases} \quad (4)$$

where  $x$ ,  $y$  is the number of agent  $G$  and  $U$  strategies.

User behaviour in social networks is a type of dynamic interaction that evolves continuously throughout the development process. The main characteristics of social networks are reflected in user engagement behaviours. Identify node attributes, investigate social network secret nodes, identify viral marketing influencers, and investigate node centrality. Exploring secret nodes is crucial in complicated social networks because it can help detect terrorists sooner, recommend certain things to potential buyers, and uncover origins of misinformation.

## 7. Conclusion

This work gives a survey on the existing psychology of trust mechanisms. Describe the trust and trustworthiness with respect to various domains such as social networks, computerised systems, economics, etc. Review the various trust management techniques in cloud computing, cryptography and machine learning. Also discussed the trust evaluation methods that are categorised as bioinspired, socio-inspired, computational and analysis-based trust. Particularly, this study categorised the existing trust evaluation methods into sub categories-based functions of different trust level calculation techniques like game theory approach, machine learning. Evaluation criteria focused on advantages and disadvantages of different trust evaluation techniques. Article focused on issues and challenges in trust management in various fields to enhance the research work.

## Author details


Ujwala Ravale<sup>1\*</sup>, Anita Patil<sup>2</sup> and Gautam M. Borkar<sup>2</sup>

<sup>1</sup> Department of Computer Engineering, SIES Graduate School of Technology, Navi Mumbai, India

<sup>2</sup> Department of Information Technology, Ramrao Adik Institute of Technology, D Y Patil Deemed to be University, Navi Mumbai, India

\*Address all correspondence to: [ujwala.ravale@siesgst.ac.in](mailto:ujwala.ravale@siesgst.ac.in)

## IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

## References

- [1] Fan X, Liu L, Zhang R, Jing Q, Jing Ping B. Decentralized trust management: Risk analysis and trust aggregation. *ACM Computing Survey*. 2019;53(1):1–33. Article ID: 2
- [2] Balaji PG, Srinivasan D. An introduction to multi-agent systems. In: *Innovations in Multi-Agent Systems and Applications*. SCI, Springer; 2010; 310:1–27
- [3] Jones Granatyr, Vanderson Botelho, Otto Lessing, Edson Emilio Scalabrin, Jean-Paul Barthes. Trust and reputation models for multi-agent systems. *ACM Computing Surveys*. 2015;(2):1-42
- [4] Pinyol I, Sabater-Mir J. Computational trust and reputation models for open multi-agent systems: A review. *Artificial Intelligence Review*. 2013;40:1-25
- [5] Sherchan W. A survey of trust in social networks. *ACM Computing Surveys*. August 2013;45(4):1-33. Article ID: 47
- [6] Jiang W, Wang G, Bhuiyan ZA, Jie W. Understanding graph-based trust evaluation in online social networks: Methodologies and challenges. *ACM Computing Surveys*. March 2017;49(1):1-35. Article ID: 10
- [7] Keum DH, Lim J, Ko Y-B. Trust based multipath QoS routing protocol for mission-critical data transmission in tactical ad-hoc networks. In: *Security and Privacy in Wireless Sensor Network (Basel)*. June 2020;20
- [8] Ali A, Ahmed M, Khan A, Ilyas M, Razzaq MS. A trust management system model for cloud. In: *International Symposium on Networks, Computers and Communications (ISNCC)*. 2017
- [9] Kerrache CA, Calafate CT, Cano J-C, Lagraa N, Manzoni P. Trust management for vehicular networks: An adversary-oriented overview. *IEEE Access*. 2016
- [10] Cho J-H, Swami A, Chen I-R. A survey on trust management for mobile Ad Hoc networks. *IEEE Communications Surveys & Tutorials*. 2011
- [11] Wang Y, Cai Z, Yin G, Gao Y, Tong X, Han Q. A game theory-based trust measurement model for social networks. *Computational Social Networks*. 2016
- [12] Wang J, Qiao K, Zhang Z. Trust evaluation based on evidence theory in online social networks. *International Journal of Distributed Sensor Networks*. 2018;14(10)
- [13] Chen X, Yuan Y, Lu L, Yang J. A multidimensional trust evaluation framework for online social networks based on machine learning. *IEEE Access*. 2019;7
- [14] Peng Z, Rastgari M, DorostkarNavaei Y, Daraei R, Oskouei RJ, Pirozmand P, et al. TCDABCF: A trust-based community detection using artificial bee colony by feature fusion. *Hindawi, Mathematical Problems in Engineering*. 2021;2021
- [15] Liu S, Zhang L, Yan Z. Predict pairwise trust based on machine learning in online social networks: A survey. *IEEE Access*. 2018;4
- [16] Mohammadi A, Golpayegani SAH. SenseTrust: A sentiment based trust model in social network. *Journal of Theoretical and Applied Electronic Research*. 2021
- [17] Mayadunna H, Rupasinghe L. A trust evaluation model for online social networks. In: *National Information*

Technology Conference (NITC); IEEE. 2018

[18] Guangchi Liu, Chenyu Li, Qing Yang, “NeuralWalk: Trust assessment in online social networks with neural networks”, INFOCOM—IEEE Conference on Computer Communications, 2019.

[19] Khalil A, Mbarek N, Togni O. Fuzzy Logic based security trust evaluation for IoT environment. IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA). 2019

[20] Kesarwani A, Khilar PM. Development of trust-based access control model using fuzzy logic in cloud computing. The Journal of King Saud University: Computer and Information Sciences. Part A. 2019;**34**(8):4956-4967

[21] Anita X, Bhagyaveni MA, Manickam JML. Fuzzy-based trust prediction model for routing in WSNs. Hindawi Publishing Corporation Scientific World Journal. 2014;**2014**. p. 11. Article ID: 480202

[22] Mujawar TN, Bhajantri LB. Behaviour and feedback-based trust computation in cloud environment. Journal of King Saud University: Computer and Information. September 2020;**34**(8):4956-4967

[23] A Boukerche, Xu L, An agent-based trust and reputation management scheme for wireless sensor networks, IEEE Conference and Exhibition on Global Telecommunications (GLOBECOM), 2005.

[24] Kumar M, Kulkarni AJ. Socio-inspired optimization metaheuristics: A review. Socio-cultural Inspired Metaheuristics. Studies in Computational Intelligence. Springer. 2019;**828**:241–265

[25] Shpak M, Kichuk A, Sytnyk O, Ishchuk N, Filonenko D, Hrozna O.

Socio-psychological factors of user trust in information in electronic mass communication. Special Issue: Innovation in the Economy and Society of the Digital Age. 2021;**39**(5)

[26] Trcek D. Computational trust management, QAD, and its applications. Informatica. March 2014;**25**(1):139-154

[27] Gokulnath K, Uthariaraj R. Game theory based trust model for cloud environment. Hindawi Publishing Corporation, e Scientific World Journal. 2015;**2015**:10. Article ID: 709827