International Journal of Advanced Culture Technology Vol.6 No.1 .32-41 (2018)
https://doi.org /10.17703/IJACT.2018.6.1.32

IJACT 18-1-5

Trust-based business model in trust economy: External interaction, data orchestration and ecosystem value

Song, Minzheong†

Department of Media & Advertising, Hansei University, Korea
mzsong@hansei.ac.kr

Abstract

The aim of this study is to formulate a trust-based business model of Internet services in so called the "trust economy." For it, firstly concepts of trust and trust economy are discussed. Then, we present previous literatures' review of trust in social science prism and trust economy in economic prism. This study classified the literatures' stances with two viewpoints of the 'system' and the 'user'. With this backdrop, we discuss three contradictory stances: Internal optimization vs. external interaction, personal data control vs. orchestration, and end-user vs. ecosystem value. In the result, we formulate a trust-based business model framework with three trust issues in user perspective and suggests three strategic directions related three issues along with representative use cases.

Keywords: *Business model, Internet service, Trust economy*

1. Introduction

Information and communication technology (hereafter ICT) convergence is taking place in innovation of the mobile communication & device, and cloud computing. The customer ownership is changing from the legacy to start-up companies who understand the customer well in terms of convenience and simplicity. As the dependence on Internet services becomes ever more essential in every aspect of human life, people understand, ICT is any method of communication, hardware or software, mobile phone or web and convergence is assistance in delivering enriched experiences for consumers. ICT convergence is the ability of different computing devices, services, or networks to provide different services over a common platform. It brings industries in the ICT sector together, which were viewed as distinct in commercial and technological sense. For example, IT & telecommunication industries converge for cloud services.

This is bringing together technology, market to integrate across diverse ICTs: Global common place of transaction, combination of different technology, service, business, market, culture etc. and ability to integrate many systems into one system. There needs to be a consensus toward common understanding and it can be found in many areas such as technology, market, ideas, culture, policy, business, trust, and so on. In terms of the trust, conventional security focus has shifted to user privacy focus. Traditional ICT requires people to adapt to systems, but new systems are designed to cater people's personal needs. These are related to the issues of data and privacy. There is a bargaining between data and privacy. Personal data is related to an individual. It

Manuscript Received: February 3, 2018 / Revised: February 15, 2018 / Accepted: February 27, 2018
Corresponding Author: mzsong@hansei.ac.kr
Tel:+82-31-450-5028, Fax: +82-31-450-5187
Department of Media & Advertising, Hansei University, Korea

is identified data with an individual. Privacy is the ability of the individuals to seclude their information.

This study is interested in a trust based business model of Internet service. Technology enablers and global price competition have hindered revenue growth and not only the legacy operators, but the start-ups also need to find new business models to drive profitable growth and justify continued investment. Internet users need to follow some practices to protect themselves and many business model opportunities in it exist on basis of the trust relation between the operator and the user. The purpose of this study is to suggest the trust based business models of Internet services. For it, it will discuss the concept of trust and search literatures about trust with viewpoints of 'system' and 'user'. With this, it will formulate a business model framework and discuss the three business strategies for developing trust embedded Internet services.

2. Definition of trust and previous reviews

2.1 Concept of trust

Trust is related to the emotion and in social contexts, trust has several connotations [1]. Definitions of trust [2][3] typically refer to a situation characterized by the following aspects: One party (trustor) is willing to rely on the actions of another party (trustee); the situation is directed to the future. In addition, the trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee. As consequence, the trustor is uncertain about the outcome of the other's actions; they can only develop and evaluate expectations. The uncertainty involves the risk of failure or harm to the trustor, if the trustee will not behave as desired. Vladimir Ilych Lenin expressed this idea with the sentence "Trust is good, control is better" [4].

Trust has been studied in many academic disciplines. Scholars tend to categorize the trust. For instance, McCullagh [5] defines three types of trust: Behavioral, business, and technology, while Kini & Choobineh [6] make a distinction from three different perspectives on trust: Individual, societal and relationship. The relationship is an important keyword in trust economy. Trust is relationships among people. It can be demonstrated that humans have a natural disposition to trust and to judge trustworthiness that can be traced to the neurobiological structure and activity of a human brain. Some studies indicate that trust can be altered e.g. by the application of oxytocin [7] . Trust is also attributable to relationships within and between social groups (history, families, friends, communities, organizations, companies, nations, etc.). It is a popular approach to frame the dynamics of inter-group and intra-group interactions in terms of trust [8]. When it comes to the relationship between people and technology, the attribution of trust is a matter of dispute. The intentional stance demonstrates that trust can be validly attributed to human relationships with complex technologies. However, rational reflection leads to the rejection of an ability to trust technological artefacts [9] .

One of the key current challenges in the social sciences is to rethink how the rapid progress of ICT has impacted constructs such as trust. This is specifically true for information technology that dramatically alters causation in social systems. In sociology degree to which one party trusts another is a measure of belief in the honesty, fairness, or benevolence of another party. The term "confidence" is more appropriate for a belief in the competence of the other party. In economics trust is conceptualized as reliability in transactions. In all cases trust is a heuristic decision rule, allowing the human to deal with complexities that would require unrealistic effort in rational reasoning. In real world "brick & mortar economy", when signing a contract, people will probably rely on some form of bank issues credentials like credit card. For sure, they will attach trust to this identity card. The credit card with its pin is a good proxy for the identity.

In fact, without uncertainty, trust is not an issue, because certainty means that the outcome will be the same, whether trusting act was involved or not. So, "the trust is not a relation itself but a second order property qualifying first order relation" [10]. Therefore, trust in connected online world is also an instance of this second-order nature and is the dominating element of the online communications. Important is that the

common factor of offline and online trust is that both are based on the trustee's trustworthiness and that transparency and honesty is the trust's main natures. But one big difference is that online world is global. Especially, establishing the identity is made very difficult, because there are no central bodies in the world. Therefore, the one of the main trust natures should be the good intention.

2.2 Previous reviews in social and economic sense

Trust has been studied in disciplines in sociology [11] [12] [13], psychology, economics [14], and computer science [15] [16] and the question before reviewing literatures is how people can establish trust on the Internet, in online world. Many disciplines have defined from different perspectives and all can't be applicable to Internet services. Therefore, this study is dealing with perspectives of the online trust in trust economy.

Online trust can be classified into two perspectives: 'system' and 'user'. The first comes from the security [17]. It is "the expectation that a system will faithfully behave in a particular manner to fulfill its intended purpose". For example, a computer is trustworthy if its software and hardware can be depended on to perform as expected, such that its services are still available, unaltered, and behave in the same way as they did yesterday [18]. The system trust is supported by software- [19] and hardware-based solutions [20]. In information security, computational trust is the generation of user trust through cryptography. It is the expectation that a system faithfully behaves to fulfill its intended propose. Usually, in centralized systems, security is based on the authenticated identity of external parties and the system trust is supported by software and hardware based solutions. However, the latter comes from sociology, with "a subjective expectation an entity has about another's future behavior" [21] [22]. In online sites like Amazon, trust is based on the feedback on past interactions between members [23] [24]. As two members interact each other, their relationship can be strengthened. The trust increases between members if the experience is positive. In the user perspective, trust has two types: direct and recommendation trust. Direct trust is based on the direct experience of the member with the other party and recommendation trust is based on experiences of other members with the other party.

Based on two different viewpoints, Momani and Challa [25] reviewed the treatment of trust in wireless and sensor network domains and Suryanarayana and Taylor [26] reviewed trust management in P2P applications, classifying it into three categories of credential and policy based, reputation based, and social network based. The basic idea behind the credential- and policy-based trust management is to use credentials to enable a policy-based access control of the resources. The reputation based trust management system provides an ability to evaluate the trust of the resource owner based on reputation values. The social-network-based method uses social relationships to rank nodes in the network.

Trust has been studied in Internet layer from three aspects: Web content, Web application, and its services. Beatty et al. [27] conducted a study of consumer trust on e-commerce Web sites, focusing on the organization of the Web content to ensure trustworthiness. Grandison and Sloman [28] surveyed trust from the viewpoint of applications to identify trust needs for e-commerce applications and provide a comprehensive set of features required for developing a trust management system. Trust has also been studied in area of computing [29] [30], where trust plays a major role in selecting the best services for a user. Wang and Vassileva [31] reviewed various trust and reputation systems for Web service selection and propose a typology to classify them along three dimensions: centralized versus decentralized, persons/agents versus resources, and global versus personalized. Josang et al. [32] surveyed Internet applications in which they provide an overview of existing and proposed systems that can be used to derive measures of trust and reputation for Internet transactions. Golbeck [33] reviews trust in Web content, services (in P2P networks and Web services), and applications.

The social network service (SNS) requires new approach in the study of trust and a few trust models have been developed. Sherchan, Nepal and Paris [22] categorized social trust with three criteria: trust data collection,

evaluation, and dissemination. The first has three sources such as attitudes, behaviors and experiences. The second is graph, interaction, and hybrid based. The last, the trust dissemination is divided into recommendation and visualization. The sub categories of those three criteria have been discussed. In the first, trust data collection, the attitudes come from a user's interactions and the experienced data can be implicit or explicit. Explicit ones are direct interactions. Feedback mechanisms are tools for reflection on direct experiences. Such may affect behaviors. These are identified by patterns of interactions.

In terms of the trust evaluation, Hang and Singh [34] employed a graph-based approach for measuring trust and it uses the similarity between graphs to make recommendations. Zuo et al. [35] proposed an approach for computing trust in social networks using a set of trust chains and a trust graph and this uses a trust certificate graph and calculates trust along a trust chain. Caverlee et al. [36] proposed a social trust model exploiting social relationships and feedback to evaluate trust. Liu et al. [37] proposed an approach for predicting trust in online communities using the interaction of the users.

In visualization of the trust dissemination, graphs are the strength of connection between two nodes. O'Donovan et al. [38] proposed a model that extracts negative data from the comments on eBay, computes personalized trust, and presents this data graphically. The graph shows the trust value and the trust strength calculated based on the number of transactions/comments between two users. Guerriero et al. [39] proposed a trust-based visualization of cooperation context between members and Bimrah et al. [40] proposed a visualization language for trust-related requirements elicitation. Recommendation involves constructing a trust network where nodes are users and edges represent the trust placed on them. Hang et al. [34] used a graph-based approach to recommend a node in a social network using similarity in trust networks. Massa and Aversani [41] also proposed a trust-based recommendation system where it is possible to search for trustable users by exploiting trust propagation over the trust network.

In economic sense, several studies have identified a lack of trust as one of the main possible constraints on Internet economy and other worries that focus on three trust issues in electronic commerce(e-commerce): identity, privacy and security. Trust strategies have been developed and some are suited to meeting the demands of the Internet economy: Identity, third-party certification, loss insurance and legal frameworks [42]. It is important to establish the authentication of the consumer by the supplier in system perspective and trust in the reputation of the supplier by the consumer in user perspective. One way to establish the consumer's identity is through use of a verifier. But, the use of authentication impacts privacy, as the verifier must maintain records of requests for verification, if a dispute arises. Third-party certification can provide data that goes beyond the identity of an agent, for instance using products providing data on aspects like reputation and signals of external approval. VeriSign secure seal is an example. In the case of voluntary use of this seal, the amount of data disclosed to the third party is clearly specified within defined limits and holders of the certification can control the publication of data, so privacy is not a major concern.

When certification is involuntary, companies may feel that their feel that the confidentiality of commercially-sensitive data has been compromised. Loss insurance limits the potential damage caused to a consumer in transactions. This reduction reduces the level of trust required to engage in a transaction has the effect of enhancing guaranteed trust transactions. The direct impact of loss insurance on Internet usage is illustrated by the way the U.S. Electronic Funds Transfer Act, which limited consumer losses in electronic transactions to $50 per credit card, increased electronic purchases and expanded the credit card industry. When it was enacted, banking associations assumed that such regulation would dampen the credit card market. The last legal frameworks reduce temptation by making illegal activities expensive, and different regulatory and legal frameworks can address different trust concerns [42].

3. Discussion of three contradictory trust stances

3.1 Internal optimization vs. external interaction

The trust data collection [22] has characteristics like transparency, experience, and reputation coming from the attitudes and behaviors. The transparency and the honesty are the two of trust's main features. Experience is the knowledge of an event gained through involvement in it and there are two types: Physical experience occurs whenever an environment changes and mental one involves aspects of intellect and consciousness exp erienced as thought, perception, memory, emotion, will and imagination. Experienced data can be implicit or explicit. In Internet world, trust model is based on feedback and this is designed to capture a member's experience interacting with the other [43]. Therefore, external interaction is very important. Josang et al. [32] discuss trust model based on user experiences. Reputation based trust models utilize experience as the main source of trust data. Experience provides one aspect of trust data and needs to be considered along with the other aspects like attitudes and behaviors.

In the source stage, trust occurs in two perspectives. In system perspective, security is important for trust and traditional ICT companies are concerned with data security. The security is the expectation that a system will faithfully behave in a manner to fulfill its intended purpose. The system trust is supported by software based solutions. This is a pipeline perspective. It means, this security-based business model creates value by controlling a linear series of activities [44]. However, in user perspective, trust is based on the feedback on past interaction among users. The trust in Internet services has two types: Direct and recommendation trust as mentioned above. The latter is experiences of other members in the social network with the other party. It means, Internet trust is usually taking place by recommendation and it is connected to reputation. For instance, a user of eBay is conscious of reputation and the reputation of seller is a key factor to buy the product. In other words, eBay's reputation is an asset with a lot of value. The user perspective is coming from psychology and sociology. It is a subjective expectation that an entity has about another's future behavior.

3.2 Control vs Orchestration of personal data

The trust evaluation in Internet service can be earned by interaction and this is an action occurring as two or more objects have effect on one another. The two-way effect is essential in the concept of interaction. So, Sherchan, Nepal and Paris [22] compared the graph- and interaction-based. The former is for measuring trust in terms of computational network-based [34]. Liu et al. [37] approached the interaction of the users and there are two types of taxonomies: The user actions taxonomy is for shared data with metrics like number and frequency of reviews, number and frequency of ratings, number and length of comments given to reviews. The pair interactions taxonomy is for different possible interactions that could happen between two users, between writers and raters, writers and writers, and raters and raters, and so on. This model considered the time difference between two users' actions which form the connection and they described a supervised learning approach that automatically predicts trust between a pair of users using evidence derived from actions of individual users as well as from interactions between pairs of users.

In the process stage of the Internet service, the contradictory trust issue is "who"s control of personal data. Nowadays, several access control techniques are available, and Internet service offerings are primarily controlled by operators or providers. It is role-based control. However, they need to move from data control to orchestration for giving controllability to users. It can be earned by interaction, not by institution. Decentralized solutions allow users to have more control capability over their own data. It is a relation based control. The first trial was conducted by Amazon. While the digital cash have been managed by token suppliers, data collection process has been required. The old form of user controlled information sharing is Amazon's "Amazon Honor System" in 2001. This allows users to make voluntary payments to gain access to lots of

products and services. The user using this can be linked via a paybox to a pay page on Amazon.com, where Amazon's "one click" technology is activated to make the payment. That means, Amazon manages both, security controls and user privacy.

3.3 End-user value vs. ecosystem value

In trust dissemination, the recommendation based trust provision is important and this trust is naturally connected to the reputation. However, the problem is that reputation can't be viewed as a single value anymore, as the ecosystem is complicated. Especially, users, developers, and sellers, all members of ecosystem must be protected against various attackers for malicious intents. The attacks in Internet services can be insidious in stealing users' identity. So, it is not only the permission and authentication issue, but the protection and authorization issue. As the e-commerce is proliferating all over the world, several studies emphasized. The importance of the trust in e-commerce, particularly in electronic transactions. It requires identity issues in addition to security and privacy. For consumer, identity is bound up with personal data protection, rather than the permission of security safe guards. The trust in the business paradigm is an authorization based trust in business ecosystem is very important.

4. Trust based business model

4.1 Strategic Framework

This study firstly presented a comprehensive review of previous literatures about the Internet trust and there is a common understanding that researchers have different viewpoints to define and evaluate the trust in computer science with perspectives of system or user. The trust is treated as calculative on one side, relational on another side. Sherchan, Nepal and Paris [22] studied lots of literatures and formulated social trust model and tried to compare computational and sociological aspects. As result, the sociological aspect of trust is from user perspective and it includes emotion, behavior, attitude, and experience of the users. Influenced by the holistic model of Sherchan, Nepal and Paris [22], this study develops a strategic framework for developing trust based business models from user perspective. The trust stages are divided into source, process, and result and a strategic framework from user perspective can be formulated as the following Table 1.

Table 1. Strategic framework for trust-based business model in user perspective

Categories of each trust stage	Characteristics of user perspective	Contradictory trust issues	Trust based Biz. strategy
Source stage: Trust data collection	Transparency, experience, reputation	Internal optimization vs. external interaction	Trust management
Process stage: Trust value evaluation	Earned by interaction	Control vs. orchestration of personal data	Orchestrated data sharing
Result stage: Trust value dissemination	Reputation network	User value vs. ecosystem value creation	Authorization Management

This study is interested in understanding of security & privacy, controllability over personal data, and protection against attacks and it caught the contradictory stances as follows: Internal optimization vs. external interaction, control vs. orchestration of personal data, and end-user vs ecosystem value. Based on this, three strategic directions are suggested 'trust management' on the source, 'orchestrated data sharing' on the process and 'authorization management' on the result stage.

4.2 Strategic Direction: Trust management

In terms of the understanding of security and privacy, data security focus has been gradually moving to user privacy, for computing systems tend to be designed to satisfy people's needs, rather than to require them to adapt to systems. With regards to privacy, there are three paradoxes: Transparency, identity, and power. To extract value from data, people need analytics. Data is generated by everything around the Internet services all times. Every digital process and social media exchanges produce data. Systems, sensors and mobile devices transmit the data and it is arriving from multiple sources at velocity, volume and variety. Data is changing the way people work. But, its benefits are realized at large corporations and governments. For instance, Google started a project in 2008 that raised the possibility of up-to-the-minute flu data. "Google Flu Trends" counted flu-related searches to estimate how many people were sick. But, it has come under fire for overstating flue incidence. It showed business model potential of data from social media. Google is doing amazing things monetizing the data they have collected from people. Data promises to use the data to make the world more transparent. However, data collection is invisible and collection techniques are not clear, even hidden by layers of physical, legal, and technical privacy. For trusting such data, transparency is not enough.

The identity paradox means that data and creativity can't work well together. Through data-based characterizations, people can lose their identity and the danger is a long-term loss of creativity that the industry will certainly suffer. For example, on video streaming of Netflix, a TV series <House of Cards> debuted on Feb. 1, 2013 and it has nine out of 10 ratings in 2015. It has made TV shows based on what people like. It means, the industry designs for what people liked previously and businesses make decisions based on data. But, great art springs from risky ventures. It is the latest triumph of data mining conceived by Netflix by leveraging viewer data. It looks at what else viewers of BBC series <House of Cards> liked and it showed, viewers liked political dramas, the actor, Kevin Spacey, and Producer, David Fincher.

In terms of the power paradox, data pools are in the hands of powerful intermediary institutions, not general people. Power is consolidated in the aggressive, data-consuming companies like Google. For example, PRISM is a clandestine national security electronic surveillance program operated by the NSA (National Security Agency) since 2007. On June 2013, The NSA program uses nine Internet giants and telecommunications to collect Internet users' material, including searches, the content of emails, file transfers, IMs and live chats. Now, Microsoft, Google and Twitter publish transparency reports showing the number of worldwide government requests they receive for user information and content.

There are two types dealing with user privacy: Giving companies more ownership over customers' data by giving free services to consumers in exchange for their data or giving consumers more ownership over their data including the potential ability to monetize it. Nowadays, people are experiencing heating privacy market and emerging needs for data protection. Consumers will probably pay to manage their privacy and choices on privacy are always contextual. The trust is a way to measure the risk in interacting within unknown services and users. Internet services should be risk free and the trust based infrastructure can build trust with consumers by defending their privacy. In the source stage, Internet service should be risk free. The trust is a way to measure the business risk in interacting with users. It is the user privacy focused. In this understanding, the strategic direction is the "trust management" to ensure the quality of services. The trust data is a tailored trust. In other words, its main characteristics are reputation and transparency. This stage is based on more social and soft approach with privacy mindset, rather than the security mindset. Trust builds business reputation and there are several business models with reputation-based trust management system: Commerce sharing (eBay), opinions sharing (Del.icio.us), jobs sharing (LinkedIn), SNS (Facebook), news sharing (Zdnet), semantic Web as for anyone who publish anything, and P2P networks where peers share opinions about other peers.

4.3 Strategic Direction: Orchestrated personal data sharing

Data sharing should focus on the user-specified privacy orchestration and the trust is a relationship-based trust rather than roll-based, because decentralized protection solutions allow users to have more control over their own data. In the process stage, the strategic direction is the "orchestrated data sharing". Decentralized solutions require orchestration mindset. According to Carminati, et. al [45], personal data is not only connected to user profiles, but spans across users' social activities and interactions. Therefore, access control techniques should be improved to be more user-centric as possible. Users and resources in Internet services are interconnected thru diverse types of relationships. Cheng, Park, and Sandhu [46] proposed a user-to-user relationship-based access control model for SNS. They developed a path checking algorithm to determine if the required relationship path between users for a given access request exists, and provided proofs of correctness and complexity analysis for this algorithm. In practice, relationship-based access control evolves with user specified policies. In Internet services, there are privacy control types such as personal, status update, location, shared-Internet networks, and so on. For instance, in LinkedIn, users can control privacy settings of online resume by themselves.

4.4 Strategic Direction: Authorization management

Members control and filter who can attack other's reputation and it requires the protection against any attack. There are several attacks which are insidious in Internet services. Digital identity is information on an entity used by computer to represent an external agent. It can be a person, organization, application, or device. The data contained in a digital identity allows the questions to be answered without the involvement of human operators. Digital identities can allow human's or device's access to computers and the services they provide to be automated, and make it possible for computers to mediate any relationships. Digital identity is used in ways that require data about persons stored in computer to be linked to their identities. That data can be used by others to discover that person's identity. Digital identity is one of the versions of a person's identity. Protection against attack should be based on the authorization mindset, rather than the authentication.

In the result stage, the strategic direction is "authorization management" in regards with the identity management. People should think not only the single-sign-on (SSO) technique, but also the several identity attacks. It needs authorization technologies.

Several attacks like malware, worms, spam, and phishing are carried out in different situations. Identity management system should give users the possibility of storing their own data where they prefer. It can reduce the user perception of security system. The open standard for authorization with OAuth2.0 is a good example. The users as resource owners can authorize limited 3rd party access to their server resources without sharing their credentials. For instance, Gmail user can allow LinkedIn to have access to their list of contacts without sharing their Gmail user name and password.

Acknowledgement

This work was supported by the ICT R&D program of MSIP/IITP. [R0190-15-2027, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system]

References

[1] D.H. McKnight and N.L. Chervany, The Meanings of Trust, Scientific report, University of Minnesota, 1996.

[2] R.C. Mayer, J.H. Davis, and F.D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review,* Vol. 20, No. 3, pp. 709-734, 1996.

[3] W. Bamberger, "Interpersonal Trust - Attempt of a Definition. Scientific report," Technische Universität München. Retrieved on Aug. 16, 2011.
[4] A.B. Seligman, "On the limits of Confidence and Role Expectations," *American Journal of Economics and Sociology,* Volume 57, Issue 4, pp. 391–404, October 1998.
[5] A. McCullagh, "Trust, Contract and Economic Cooperateion," *Cambridge Journal of Economics,* Vol. 23, pp 301-315, 1998.
[6] A. Kine and J. Choobineh, "Trust in Electronic Commerce; Definition and Theoretical Considerations," in W. Blanning and D. King(eds.), *Proceeding s of the 31 Annual Hawaii Conference on System Sciences,* Volume IV, IEEE Computer Society, 1998.
[7] M. Kosfeld, M. Heinrichs, P.J. Zak, U. Fischbacher, and E. Fehr, "Oxytocin increases trust in humans," *Nature435,* pp. 673-676, 2005.
[8] R. Hardin, (eds.), Trust and trustworthiness. Russell Sage Foundation, 2002.
[9] B. Shneiderman, "Designing trust into online experiences," *Communications of the ACM*, Volume 43, Nr.12. pp. 57-59, 2000.
[10] M. Taddeo, "Defining trust and e-trust," in: A. Mesquita, Sociological and Philosophical Aspects of human interaction with technology, Information Science Reference, pp. 23-25, 2011.
[11] D. Helbing, "A mathematical model for the behavior of individuals in a social field," *J. Math. Sociol.,* Vol. 19, Nr. 3, pp. 189-219, 1994.
[12] G. Mollering, "The nature of trust: From geog simmel to a theory of expectation, interpretation and suspension", *Sociol.*, Vol. 35, pp. 403-420, 2002.
[13] L.D. Molm, N. Takahashi, and G. Peterson, "Risk and trust in social exchange: An experimental test of a classical proposition," *Amer. J. Sociol.,* Vol. 5, Nr. 105, pp. 1396-1427, 2000
[14] F. Huang, "Building social trust: A human-capital approach," *J. Institut. Theor. Econ.*, Vol. 163, Nr. 4, pp. 552-573, 2007.
[15] M. Maheswaran, H.C. Tang, and A. Ghunaim, "Towards a gravity-based trust model for social networking systems," in *International Conference on Distributed Computing Systems Workshops. IEEE Computer Society,* Los Alamitos, CA, Sep. 24, 2007.
[16] D. Hughes, G. Coulson, and J. Walkerdine, "Free riding on gnutella revisited: The bell tolls?" *IEEE Distrib. Syst.* Online 6, Nr. 1, 2005.
[17] J. Yao, S. Chen, S. Nepal, D. Levy, and J. Zic, "Truststore: Making amazon s3 trustworthy with services composition," in *the 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGRID'10). IEEE Computer Society,* Los Alamitos, CA, pp. 600-605, 2010.
[18] D. Moreland, S. Nepal, H. Hwang, and J. Zic, "A snapshot of trusted personal devices applicable to transaction processing," *Personal Ubiq. Comput,* Vol.14, Nr. 4, pp. 347-361, 2010.
[19] A. Seshadri, A. Perrig, L. Van Doorn, and P.K. Khosla, "SWATT: Software-based attestation for embedded devices," in *the IEEE Symposium on Security and Privacy*, pp. 272-282, 2004.
[20] L. Chen & J. Li, "Revocation of direct anonymous attestation," in *the 2nd International Conference on Trusted Systems (INTRUST'10)*, pp.128-147, 2010.
[21] L. Mui, *Computational models of trust and reputation: Agents, evolutionary games, and social networks,* Ph.D. thesis, http://groups.csail.mit.edu/medg/people/lmui/docs/phddissertation.pdf., 2003.
[22] W. Sherchan, S. Nepal, and C. Paris, "A Survey of Trust in Social Networks," *ACM Computing Surveys,* Vol. 45, Nr. 4, Article 47, Aug. 2013.
[23] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems," *Comm. ACM,* Vol. 43, Nr. 12, pp. 45-48, 2000.
[24] S. Ruhomaa, L. Kutvonen, and E. Koutrouli, "Reputation management survey," in *the 2nd International Conference on Availability, Reliability and Security (ARES'07)*, IEEE Computer Society, pp. 103-111, 2007.
[25] M. Momani & S. Challa, "Survey of trust models in different network domains," Int. J. Ad Hoc Sensor Ubiq. Comput., Vol. 1, Nr. 3, pp. 1-19, 2010.

[26] G. Suryanarayana & Taylor. R., "A survey of trust management and resource discovery technologies in peer-to-peer applications," Tech. rep. UCI-ISR-04-6, Institute for Software Research, University of California, Irvine, 2004.
[27] P. Beatty, I. Reay, S. Dick, and J. Miller, "Consumer trust in e-commerce web sites: A metastudy," *ACM Comput. Surv.,* Vol. 43, Nr.2, pp. 1-46, 2011.
[28] T. Grandison & M. Sloman, "A survey of trust in Internet applications," *IEEE Comm. Surv. Tutorials* 3, Nr. 4, 2000.
[29] Z. Malik, I. Akbar, and A. Bouguettaya, "Web services reputation assessment using a hidden markov model," in *the 7th International Joint Conference on Service-Oriented Computing (ICSOCServiceWave'09),* pp.576-591, 2009.
[30] E. Chang, T.S. Dillon, and F. Hussain, "Trust and Reputation for Service-Oriented Environments: Technologies for Building Business Intelligence and Consumer Confidence," *Wiley Periodicals,* 2006.
[31] Y. Wang & J. Vassileva, "A review on trust and reputation for web service selection," in *the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07). IEEE Computer Society,* pp. 25–32, 2007.
[32] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decis. Support Syst.,* Vol. 43, Nr. 2, pp. 618-644, 2007.
[33] J. Golbeck, "Trust on the World Wide Web: A survey," *Found. Trends Web Sci.* Vol. 1, Nr. 2, pp. 131-197, 2006.
[34] W.C. Hang & M.P. Singh, "Trust based recommendation based on graph similarities," http://www.csc.ncsu.edu/faculty/mpsingh/papers/mas/aamas-trust-10-graph.pdf., 2010
[35] Y. Zuo, W.-C. Hu, and T, O'Keefe, "Trust computing for social networking," in *the 6th International Conference on Information Technology: New Generations,* IEEE Computer Society, Los Alamitos, CA, pp. 1534-1539, 2009.
[36] J. Caverlee, L. Liu, and S. Webb, "Socialtrust: Tamper-resilient trust establishment in online communities," in *the 8th ACM/IEEE-CS Joint Conference on Digital Libraries (JCDL'08).* ACM Press, New York, pp.104–114, 2008.
[37] H. Liu, E.-P. Lim, H.W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y.A. Kim, "Predicting trusts among users of online communities: An epinions case study," in *the 9th ACM Conference on Electronic Commerce (EC'08)*, ACM Press, New York, pp. 310-319, 2008.
[38] J. O'Donovan, B. Smyth, V. Evrim, and D. Mcleod, "Extracting and visualizing trust relationships from online auction feedback comments," in *the 20th International Joint Conference on Artificial Intelligence*, Morgan Kaufmann Publishers, San Francisco, pp. 2826-2831, 2007.
[39] A. Guerriero, S. Kubicki, and G. Halin, "Trust-oriented multi-visualization of cooperation context," in *the 2nd International Conference in Visualisation (VIZ'09),* IEEE Computer Society, Los Alamitos, CA, pp. 96-101, 2009.
[40] K.K. Bimrah, H. Mouratidis, and D. Preston, "Modelling trust requirements by means of a visualization language," in *the Conference on Requirements Engineering Visualization (REV'08),* IEEE Computer Society, Los Alamitos, CA, 26–30, 2008.
[41] P. Massa & P. Aversani, "Trust-aware recommender systems," in *the 1st ACM Conference on Recommender Systems (RecSys'07),* ACM Press, New York, 2007.
[42] G.A. Guerra, D.J. Zizzo, W.H. Dutton, and M. Peltu, "Economics of Trust in the Information Economy: Issues of Identity, Privacy and Security," Oxford Internet Institute, Research Report No.1, April 2003.
[43] Y. Wang, Y. Hori, and K. Sakurai, "Economic-inspired truthful reputation feedback mechanism in p2p networks," in *the 11th IEEE International Workshop on Future Trends of Distributed Computing Systems,* pp.80–88, 2007.
[44] M.W. Van Alstyne, G.G. Parker, and P.G. Sangeet, "Pipeline, Platforms, and the New Rules of strategy," *HBR.org.,* April 2016.
[45] B. Carminati, E. Ferrari, and M. Viviani, "Security and Trust in Online Social Networks," in *Synthesis Lectures on Information Security, Privacy, and Trust*, Morgan & Claypool Publishers, 2014
[46] Y. Cheng, J. Park, and R. Sandhu, "Relationship-based access control for online social networks: Beyond user-to-user relationships," in *2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing,* 2012.