A Holistic Review on Trust and Reputation Management Systems for Digital Environments

Ilung Pranata
Faculty of Science and IT
University of Newcastle
Callaghan, Australia
Ilung.Pranata@newcastle.edu.au

Geoff Skinner, Rukshan Athauda
Faculty of Science and IT
University of Newcastle
Callaghan, Australia
[Geoff.Skinner, Rukshan.Athauda]@newcastle.edu.au

***Abstract*— Digital environments have generated tremendous benefits for various entities. Individuals and organizations have utilized these environments for performing transactions, sharing information, and engaging in collaboration. However, the benefits that digital environments offer also attract a number of dishonest entities. These entities perform malicious activities that further disadvantage other genuine entities. In order to mitigate this issue, a method to investigate the trustworthiness of entities in digital environments is needed prior to any transaction or collaboration. Such method should allow entities to gauge the trustworthiness of other entities. Therefore, this method could increase the confidence of the entities to perform the transaction or collaboration. In this paper, we focus at providing a holistic review on the current state of art in trust and reputation management system. Several existing works in trust models are discussed. In addition, several requirements for an appropriate trust model for digital environments are presented.**

Trust; Reputation; Digital Environments; Trust Model

I. INTRODUCTION

One critical factor that highly influences the likelihood of entities to interact and transact in digital environments is trust. Trust is crucial that it affects the appetite of an entity to consume a particular service or product offered by another entity. This example can be seen in our everyday life where trust decisions are made. When purchasing a specific product, we may favor certain brands due to our trust that these brands will provide excellent quality compare to the unknown brands. Trust on these brands may come from our past experience of using these brands' products (termed "belief") or from their reputations that are perceived from other people, such as families and friends (termed "reputation").

Similarly, trust also affects the decision of an entity to transact with other entity in online environment. Authors in [1, 2] further stress the importance of trust for the success implementation of any online environment. Both consumers and providers in an electronic market must trust each other before decisions to consume or to provide the services are made. If trust is not established between them, fraudulent transactions may occur regularly. Such situation would disadvantage the honest consumers and providers, and it further refrain them from taking the advantage of the online transactions. The significance of trust also applies in digital environments where a high number of entities mutually interact with each other to provide and consume the information and/or resources.

Although the significance of trust in our physical world is as important as it is in the digital environments, building trust and confidence in the latter is much more difficult. This is due to our inability to have the physical view on an entity, unlike in our physical world where we can view the building of the bank, observe its safe deposits, meet the bank personnel, etc. Another issue with trust is that it is difficult to quantify the exact trustworthiness value of an entity. This is even harder when each entity have different interpretation and perception of the term "trustworthy". Therefore, they may assign different trustworthiness values for a provider or a service. For example, a service consumer assigns "very trustworthy" to the provider for a transaction that he has performed. However, another consumer assigns "untrustworthy" for the similar transaction from the same provider. These differences further increase the difficulty to determine the exact trustworthiness of a provider.

This paper discusses several existing works in trust and reputation management system from literature. The main objectives are to provide fundamental knowledge on trust for digital environments. The remainder of this paper is organized as follow. Section II lists all sources in which scientific publications are drawn. Section III provides an overview of digital environments. Section IV discusses the notion and characteristics of trust. This is followed by section V which details the elements of trust. Section VI present several existing works in trust and reputation management systems. Section VII presents several requirements for trust model in digital environments. This is followed by section VIII that concludes this paper.

II. METHOD

This paper reviews scientific publications in the area of trust and reputation management from some of the leading digital libraries. Some of the libraries in which the scientific publications were obtained are: IEEE Explore, ACM Digital Library, Springer, and Elsevier. The review also considers reviewing trust and reputation management systems from several electronic environments, i.e. peer-to-peer, e-commerce, grid computing, distributed system, and multi-agent system. The review on these electronic environments provides fundamental knowledge on the current state of research in trust and reputation management.

III. Overview of Digital Environments

Digital Environments (DEs) are viewed as the enabler and imperative technology for today transactions, collaborations, service delivery and information sharing. A large number of organisations have been involved in DEs for conducting and enabling their businesses. Authors in [3] argued that organisations that adopted DEs have improved their productivity in the following ways: (i.) operation efficiencies through automation of transactions, (ii.) greater economic advantages through intermediaries' reduction in the value chain, (iii.) consolidation of supply and demand through organised exchange, (iv.) improved marketing strategies and product/service innovation. Such potential benefits have attracted high number of enterprises ranging from small to large enterprise to take advantages of DEs. However, DEs have come a long way through the evolutions that are driven by ICT advancements and changing business environments. Hence, in this section, we present the past development of Digital Environments, the current state of DEs and also the future that DEs will hold from several literature studies. This is to provide knowledge on the advantages that DEs offer in each evolution stage and more importantly, to provide understanding on DEs' adoption by the enterprises.

Digital Environments have evolved and have gained significant progressions in the past decades. Such evolution is evidential from their first introduction in the forms of e-mail and website to nowadays computing technologies such as e-commerce, peer-to-peer, collaborative environment, distributed environment, mobile agents, cloud computing etc. Authors in [4] reveals a discussion paper that shows various DEs evolution phases and its adoption by the Small and Medium Enterprises (SMEs), in particular the European SMEs. There are two inferences that can be drawn from this paper. First, the ICT adoption in European SMEs has been historically low over the various stages despite of the significant positive impacts that ICT provide for the businesses. This is due to the digital divide issues in which the larger enterprises have skills, knowledge and investments for adopting ICT while the majority of SMEs do not have it. Second, several distinctions in the conceptual model and usage of various DEs evolution phases can be established.

The first (e-mail) and second (website) phases that took place in the past decades showed that the proliferation of electronic platforms were restricted only for information sharing. The third phase (e-commerce) started to gain momentum in utilizing the internet for performing business transactions and collaborations for the enterprises and consumers. However, this phase suffered from information fragmentation due to lack of systems integration. The fourth DEs evolution phase (e-business), which where we are right now, promotes the seamless interchange of information and interoperability between platforms. This allows ICT to link different business systems as well as modifying the working process and culture of the organizations. ICT system for Supply Chain Management (SCM) [5] is an example of this phase. Furthermore, a number of specialized digital environments have appeared in this phase in order to cater for the specific needs. Examples of these specialized digital environments are peer-to-peer environment, collaborative environment, mobile agent, cloud computing, etc.

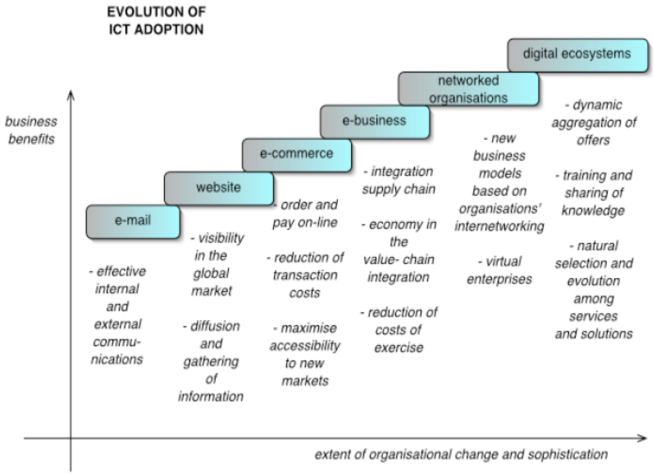
EVOLUTION OF ICT ADOPTION
business benefits
extent of organisational change and sophistication
e-mail
website
e-commerce
e-business
networked organisations
digital ecosystems
- effective internal and external commu-nications
- visibility in the global market
- diffusion and gathering of information
- order and pay on-line
- reduction of transaction costs
- maximise accessibility to new markets
- integration supply chain
- economy in the value- chain integration
- reduction of costs of exercise
- new business models based on organisations' internetworking
- virtual enterprises
- dynamic aggregation of offers
- training and sharing of knowledge
- natural selection and evolution among services and solutions

Figure 1 DEs evolution phase (Adapted from [3])

Although the fourth phase provides significant positive impacts for the organizations, the adoption of this phase is limited to the large enterprises due to the aforementioned digital divides issues. Therefore, the fifth and final DEs evolution phases are envisioned between now and the future alongside with the advancement of ICT. In these phases, organizations autonomously foster tight integration with others by rapidly building the partnership and alliances, integrating their business processes, and sharing their knowledge and expertise. Authors in [6] refer these types of organizations as the networked organizations in which businesses and organizations collaborate together for a common purpose. Such collaborations are fostered by removing organization boundaries and by continually adopting with the changes. The structure of these organizations is fluid and transient in which the partnership or alliance dissolves once the common goal is met, and any independent organization may create another alliances with other organizations that were or were not involved in the previous ones. In order to achieve this fourth and final phases, the ecosystem must be filled in with various autonomous applications and services, high amount of knowledge transfer, and business processes integration [4]. These are the major conceptual model, purpose and objective that differentiate DEs in the future from the current internet technology.

The number of literature [7, 8] reveals several characteristics that formulate the concept of the current and future digital environments. The characteristics are explained below to provide a conceptual understanding of DEs.

- Interaction and engagement, this refers to the interaction between individuals and organisations inside a digital environment. They are encouraged to engage each other towards goals, maintaining the stability of the environment and sharing resources and knowledge in a proactive and responsive manner.

- Open and distributed, this indicates a free harmony relationship among components in maintaining the sustainability of the environment. A solitary failure may not lead to either disaster or the collapse of the whole environment. Conversely, each failure structures a new balance of the environment.
- Multi domains and loosely coupled, this means related components inside Digital Environments forming groups or alliances which share similar identities, objectives and interest. These groups/alliances involve in free and open relationships which are not heavily dependent towards each other and failure on one group does not heavily affect other groups or the whole environment.
- Self-organisation, this refers to the ability of each component to act autonomously, make its own decisions, self-empowered and independent from others.
- Structural determinism, this signifies the change and evolution process of components are established from preceding component structure and stimulated by the environment.
- Structural coupling, this indicates the close connection, relation and interaction between components inside the environment creating a beneficial mutual interdependence between the entities.

One major characteristic of high performing DEs is decentralised architecture. Authors in [9] argued that due to the fluid and transient organisation structure, DEs should minimize the single point control. Thus, organisations in a DE environment could easily form alliances with others and remain flexible throughout the collaborations. Such decentralised environment also limits the single point failure in which the failure of an entity or an alliance would not disturb the entire environment. Another important characteristic of DEs is the proliferation of alliances, or virtual communities in most literature [10], [11]. Virtual communities bring together individuals and organisations with a shared purpose, interest, or goal to collaborate and learn by destroying the physical barrier and organisation boundary. Entities or members in virtual communities must remain proactive to share their knowledge and information to the others. Note that besides actively sharing knowledge and information, it is also possible that the entities may engage in active transactions with others.

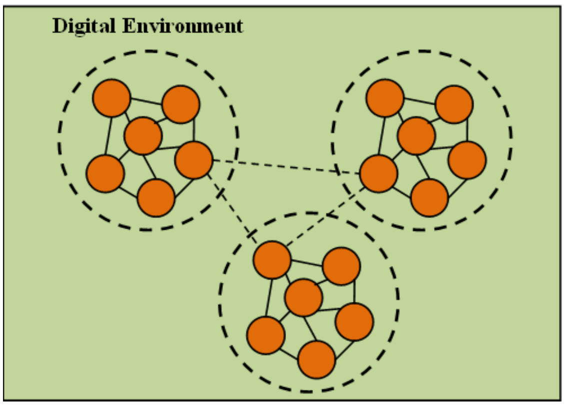

Figure 2 Decentralised and multi-domain DE

DEs also encompass several characteristics of Collaborative Virtual Environment (CVE) [12]. CVE is a platform that allows distributed teams and knowledge workers in an organisation to collaborate and share knowledge across the departments. To achieve such objective, CVE leverages ICT advances in communication technology and video processing. Several applications and technologies that are commonly utilised in CVE [13] include: 1) Communication Technology: email, video conferencing, instant messaging, 2) Resource Sharing and management: collaborative workspaces, document management, task workflow management, and 3) Knowledge sharing: blogs, wikis, bulletin boards. These applications and technologies overcomes the time and space differences as they allows distributed workers in an organisation to access and update the information at any time and from any place. Similarly, in digital environments, any entity has a freedom and should be encouraged to collaborate and share information and knowledge with another. It is important to note that while CVE is constraint to individuals (workers) within an organisation, the DEs allows collaborations across enterprises that are not restricted to single organisation.

IV. The Notion and Characteristics of Trust

A. The Notion of Trust

It is challenging to concisely define "trust" of an entity due to its uniqueness to each individual entity. Several authors in [14, 15] attempt to define trust from a sociological point of view. They define trust as the trusting behaviour that one person has on another person in a situation where an ambiguous path exists. In such definition, trust is used to mitigate the risks of the dealings with others. Other authors in [10] further define trust as the capacity and belief of an entity that the other entity would meet its expectations. However, one of the most prominent works that attempt to derive the notion of trust and was used by many research in online environment is conducted by Gambetta et al. [16]. The authors state that someone is deemed as trustworthy, subject to the probability that he will perform a particular action that is beneficial or non-detrimental for us. This definition is further extended by incorporating the notion of competence along with the predictability [17]. Gambetta et al. definition on trust is also supported by the author in [1] which further defines trust in an electronic forefront as the competency belief that an agent would act reliably, dependably and securely within a given context. This belief can be quantitatively derived from a subjective probabilistic that an agent has over another in a given period of time. We refer to this definition when discussing about trust throughout this thesis.

Trust in an electronic network can be divided into two types: direct (personal) trust and third party trust [18]. Direct (personal) trust is a situation where a trusting relationship is nurtured by two entities. This type of trust is formed after these entities have performed transactions with each other, e.g. entity

A inherently trusts entity B after a number of successful transactions that involved both entities. On the contrary, third-party trust is a trust relationship of an entity that is formed from the third party recommendations. This means no previous transaction ever occurred between the two interacting entities. For example, entity A trusts entity B because B is trusted by entity C. In this example, entity A derives trust of B from C, and A also trusts entity C does not lie to him. As with any types of trust relationship, there is a link with the risk. Risk is not within the scope of this thesis however, it is important to note that risk affect the trusting relationship between the entities. Author in [19] stresses that an entity will only proceed with the transaction if the risk is perceived as acceptable.

B. *Trust Characteristics*

There are several important characteristics of trust that further enhance our understanding about trust relationship in digital environments. Based on our review of the following literature [1, 19, 21, 22], we further observe these important characteristics of trust:

- Trust is dynamic as it applies only in a given time period. As time passes, the degree of trust on oneself may change. For example, for the past 1 year Alice highly trusts Bob. However, this morning Alice found that Bob lied to her, therefore Alice no longer trusts Bob.
- Trust is context-dependent in nature that it applies only in a given context. The degree of trust on different contexts of oneself may differ significantly. For example, Alice may trust Bob to provide financial advice but not for medical advice.
- There is no full trust. Trust that an entity has over the other entity is never 100%. An entity may have different trustworthiness values given to different entities in different contexts.
- Trust is transitive within a given context. That is, if an entity A trusts entity C then entity A may trust any entity that entity C trusts in a same context. However, this derived trust may be explicit and hard to be quantified.
- Trust is an asymmetric relationship in nature. Therefore, trust is a non-mutual reciprocal in nature. It means that if entity A trust entity B, we must not conclude that entity B trust entity A

Chang et al. [23, 24] stress that the nature of trust is fuzzy, dynamic and complex. The authors further states 6 additional characteristics of trust: implicitness, asymmetry, transitivity, antonymy, asynchrony, and gravity. As the asymmetry and transitivity characteristics were previously discussed, the following explains the rest of trust characteristics:

- Implicit: It is hard to explicitly articulate the confidence, belief, capability, context and time dependency of trust.
- Antonymy: The articulation of trust context in two entities may differ based on the opposing perspective. For example, entity A trusts entity B in the context of "buying" book, however from entity B to entity A the context is "selling" book.
- Asynchrony: The time period of trusting relationship may be defined differently between the entities. For example, entity A trusts entity B for 3 years, however, entity B may think that the trust relationship only last for the last 1 year.
- Gravity: The degree of seriousness in trust relationships may differ between the entities. For example, entity A may think that its trust with entity B is important, however, entity B may think it differently.

V. Elements of Trust

When building a trust relationship between one entity and another, there are several elements that need to be considered. These elements are context, time, belief, and reputation. The combination of such elements greatly determines and affects the trustworthiness value of an entity. Figure 3 below shows four elements of trust.

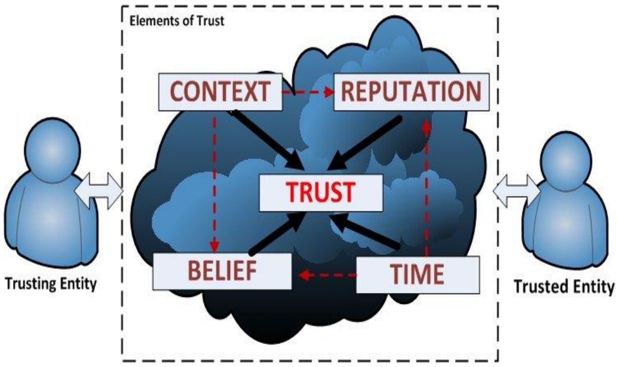

Figure 3 Elements of trust

Figure 3 presents the interdependent relationship of several elements that have a direct influence on the trust value between the entities. On the left hand, we have the trusting entity and on the right hand the trusted entity. We define the entity that is transacting with provider entity as the trusting entity**.**

Definition 1. (Trusting Entities). *Entities that are transacting with and trusting the provider entity.*

On the contrary, the provider entity that is providing services or resources is defined as the trusted entity.

Definition 2. (Trusted Entities). *Provider entities that provide resources or services to other entities.*

These definitions are used throughout this paper. The middle portion of figure 3 shows the four elements of trust. The trustworthiness value of a trusted entity is determined by the complex evaluation of belief and reputation that are within a given context and time period. The following sub-sections provide a discussion of each element that influences the trust relationship between the entities.

A. *Context & Time-Dependent*

Context provides information describing a situation or scenario, or a set of conditions of a trust relationship. Each context consists of a name, a type and a functional specification that describe a particular situation [24]. For example, in a context of borrowing a book:

- the context name is “Borrow a book”
- the context type is “Library”
- the functional specification is “Bob wants to borrow a book on Security”

Context by nature is important for the representation of a trust relationship. That is, context specifies the situations where a trust relationship is defined. It is important to understand that the degree of trust relationship between the trusting entity and the trusted entity in different contexts is not similar. For example, Alice trust Bob in the context of providing financial advice, however, Alice does not trust Bob in the context of providing medical advice. Therefore, it can be concluded that trust is context-dependent in nature in which trust that the trusting entity has on a trusted entity in a given context may not necessarily similar in another context.

Trust in a specific context is also time-dependent which represents another important element of trust. Authors in [24] classify the time-dependent of trust into three categories: time spot, time slot, and time space. Time spot is a specific time when the interaction between the trusting entity and a trusted entity occurs and a trust value is assigned. Time slot is defined as a period of duration between two time spots in which the trust values are collected. Time space is defined as the total duration of interaction between the trusting entity and a trusted entity in which all trust values of different time-slots are aggregated. The aggregated trust values will then be used to predict the future trust, or known as the trustworthiness value. Trust is dynamic in a sense that the trustworthiness value of an entity changes over the time. As the interaction between the trusting entity and a trusted entity increases over the time, the trusting entity will have a better picture on the trustworthiness of this trusted entity. The trustworthiness of a trusted entity in a transaction may decrease, increase or remain the same which further affects its aggregated trust value.

B. *Belief*

Belief in trust context refers to the trusting entity’s personal confidence on the ability of a trusted entity to meet its obligation. Furthermore, belief can also be perceived as the confidence that the trusted entity does not have any malicious intent [25]. The source of belief comes internally from a trusting entity. The belief of a trusted entity is subjective as it may differ from one trusting entity to another. A specific value could be assigned to belief in order to represent the different degree of confidence that a trusting entity has over a trusted entity. This value grows from the experience that is accumulated over the time (i.e. number of transactions that are performed by the trusting entity with a trusted entity). For example, after 100 transactions, Alice has 99% belief that Bob will deliver her purchased books on time.

As shown in figure 3, belief is bounded to context and time. The value of belief in a trusted entity may differ on multiple contexts, and it may increase or decrease over a period of time. For example, a year ago, Alice has 99% belief that Bob will deliver her books on time, but in a series of recent transactions, Bob has failed to deliver Alice’s books on time. Therefore, Alice’s belief on Bob has reduced to 70% in the context of delivering her books on time. The value of belief is highly related to the trustworthiness value of a trusted entity as it is one of the factors that contribute when deriving the total trustworthiness value. The value of belief, if present, is usually a dominant factor for determining the trustworthiness value of an entity. This is mainly due to belief is the subjective confidence and opinion that the trusting entity holds and believes from its own experience with the trusted entity. However, during the initial transaction in which the trusting entity does not have enough information to derive its own belief about the trusted entity, the other trust element that gathers the information from the community is used to determine the initial trustworthiness value of a trusted entity. Such element is defined as reputation and will be discussed in the next sub-section.

C. *Reputation*

Reputation is defined as what is generally said and believed about a person, or things character, or standing [2]. Reputation can also be interpreted as the expectation and perception that a trusting entity holds about a trusted entity from its past actions and behaviours with other entities [26-28]. For example, the reputation of Bob is computed based on the perception of Alice, John, Mark, etc. Furthermore, reputation is highly related to the measurement of trustworthiness value. That is, one can trust another based on the feedbacks of its reliability. The trustworthiness of a trusted entity is computed by aggregating all of its reputation feedbacks that are obtained from other entities. The trustworthiness value that is derived using reputation is classified as indirect or third party trust.

In E-commerce marketplaces, reputation systems have been widely utilized as trust facilitators, and also as the decision making and incentive process to avoid cheaters and frauds. The methods for computing reputation in e-commerce marketplaces are categorized into one of the following: (i) the summation of all votes that an entity receives or (ii) the average votes given to an entity. Further, most e-commerce reputation systems are centralized. That is, the reputation values (or votes) are collected and computed in central servers. eBay [29] is one of the most simplistic reputation systems amongst e-commerce sites. It uses the summation-type reputation system which is primarily based on the ratings. Another e-commerce marketplace, Amazon [30], utilizes the average-type reputation system to rate its books.

In a multi-agents system environment, reputation value is computed from a total or aggregated value of all recommendations that reports the trustworthiness of an agent [24]. These recommendations are given by several recommender agents in the environment. Several literature define the recommender agents as the witnesses who provide trust information of an entity based on their own experience or the experience gathered by others. Similar to belief, reputation is bound to context and time [24]. For example, agent Alice inquires agent John on the reputation of agent Bob in a context of providing financial advice in the last 5 years. Such example shows that reputation value of an agent is dissimilar in different contexts and time periods. Further, it is extremely crucial to note that the reputation value is collected and aggregated from a number of recommender agents whose credibility in providing honest recommendation feedback may differ from one to another. For example, extending from the previous example, agent Alice may also inquire agent Mark for the reputation of agent Bob in the same context and time period. However, agent Alice believe that agent Mark is more credible then agent John in providing honest reputation feedback about agent Bob. Thus, the recommendation feedbacks provided by both agent Mark and agent John from agent Alice's perspective may differ due to the dissimilarity of their credibility. In this example, Alice may weigh the reputation feedback given by agent Mark higher than the reputation feedback given by agent John.

VI. Review on The Existing Work in Trust and Reputation MAnagement

In this section, the current state of art in trust and reputation management systems is presented. To date, there are numerous trust solutions have been proposed for each environment (i.e. peer-to-peer, multi-agent system, e-commerce, etc.). Each of these trust solutions will be elaborated in the next sub-sections. The extensive review in this section provides fundamental knowledge on the area of trust and reputation management.

A. Early Research in Trust and Reputation Management

One of the most prominent early works in trust was presented by Abdul-Rahman & Hailes [26] that propose a model to compute entity's trustworthiness based on reputation and experience. The authors propose 5 degrees of trustworthiness as very trustworthy, trustworthy, untrustworthy, and very untrustworthy. The trustworthiness value of a provider was computed based on the summation of both entity's and recommenders' experience with him. Recommender is defined as other entities that provide feedback (recommendation) about the trustworthiness of a provider. Semantic distance is computed to evaluate the difference between the entity experience and its recommenders' experience. In this model, each entity stores the trust values of all providers that it has interacted and also its recommenders' feedback value of the providers. Such approach is considered as distributed model in which the history of past experiences and received feedbacks are stored in each entity's repository (not being accumulated in single server for all entities).

Authors in [31, 32] proposes both direct and witness approach to calculate the trustworthiness rating of a provider. The upper and lower thresholds are used to assess the trustworthy and untrustworthy parameters in a trusting relationship. This model uses the Dempster-Shafer model to calculate the 2 parameters based on multiple evidences. The referral network is used to derive provider's trustworthiness in which if the acquaintances of the requestor entity (the recommenders) do not have any information about the provider, the acquaintances will query the referrals to obtain the information. This model also specifies the depth limit of referral graph (TrustNet) to keep the referral chain restricted. However, the model does not combine direct information of an entity with its acquaintances information when computing provider's trustworthiness. If the direct information is available, then it does not use its acquaintances information.

Collaborative Filtering (CF) algorithm [33] is one of the earliest works which focus at measuring the credibility of recommendations in deriving the provider's rating. This technique generally computes the similarity measure between an entity and recommenders in the system. The similarity measure is computed by comparing entity's ratings with other entities' ratings of a set of common providers in a community. Such similarity measurement is then used to weight the recommendations of other entities. Then, CF only takes ratings from the recommenders that have the highest similarity with the entity for deriving the rating of a provider. The main focus of CF's algorithm is at deriving provider's rating using the judgments of the recommenders. A similar approach is also implemented in the modern trust model proposed by [34].

B. REGRET

Authors in [35] presents a modular trust and reputation system (REGRET) that primarily derives the trust value from three dimensions: individual dimension, social dimension and ontological dimension. The individual dimension is the direct trust between the requestor (consumer) and target (provider) entity, and it is computed from the past experience that the requestor entity has with the target entity. Social dimension computes the trust value of the target entity in relation with a group, and the ontological dimension computes the trust values based on different aspects of the target entity. Each requestor entity maintains a local database about its interaction with the target entities and it also stores the subjective evaluation (impression) on certain aspects of the target entities.

This model measures the reliability of subjective reputation based on the number and variability of impression. The social dimension is computed based on 3 criteria: (i) the aggregation of entity's previous experience with the target group, (ii) the subjective reputation of all entities in the group about the target entity, and (iii) the subjective reputation of all entities in the group about the target group. The ontological dimension is computed based on requestor entity's subjective reputations on the aspects of a target entity. For example, to compute the ontological dimension of a seller, the buyer combines all reputation values of product price, product quality, delivery date, etc. This model requires an internal database for each entity and also a centralized database to store group subjective reputation.

C. TrustMe

TrustMe [36] is a distributed approach for managing trust in a Peer to Peer (P2P) network. It utilizes a smart Public Key mechanism to preserve the anonymity of the peers. Each peer has the public-private key pair, and the trust value of a peer is randomly stored in the anonymous Trust-Holding Agent (THA) Peers. The trust value of a target peer is obtained when the request peer broadcast the query on the network and the THA peers reply to this query. The request peer then consolidates all trust values retrieved from THA peers and decide whether to interact with the target peer. TrustMe focuses on building the protocol to securely exchange trust value from any malicious peers in a P2P environment. However, the Authors do not propose any trust model for measuring the trust value of a peer in the environment and also, TrustMe does not clearly specify how trust value is updated in the THA peers.

D. EigenTrust

EigenTrust [37] is a trust model for P2P environment, and it is the most widely cited trust model in the literature. EigenTrust incorporates both local trust (direct interaction) and global trust (reputation) in its trustworthiness computations. EigenTrust measures the validity of each file in P2P as either valid or corrupt. Each peer maintains a repository that lists the trustworthiness of all peers which it has interacted before. In the absence of local trust (direct interaction) with a provider peer, a requestor peer asks other peers (recommenders) in the network to provide feedback on provider peer's trustworthiness. EigenTrust measures the credibility of feedback based on the validity of files that the recommender peers provide. That is, a peer that provides valid file is also considered credible in providing feedback and vice versa.

For bootstrapping (new peer joins the environment), EigenTrust introduces the concept of pre-trusted peers. Pre-trusted peers are the well-known peers in the environment that are notoriously known to provide credible feedback. Therefore, a new peer that does not have any experience with other peers is able to request feedback from these pre-trusted peers. Such example is seen in the real world where we tend to trust well known enterprises such as Google, Microsoft, etc. Trust computation in EigenTrust is using a normalized principal eigenvector which is a variation of Google's PageRank algorithm [38].

E. PeerTrust

PeerTrust [39] is a proposed trust model for P2P environment. It evaluates peer trustworthiness rating based on 5 important elements: (i) the feedback obtained from other peers about the target peer, (ii) the aggregated number of total transactions that the target peer has with others, (iii) the credibility factor of the recommender peers, (iv) the transaction context factor for discriminating the mission critical transaction from less or non-critical transactions, and (v) the community context factor. This model allows different weightages to be applied in different situations to each feedback based evaluation and community context evaluation. The feedback based evaluation is computed based on a number of transactions that have been conducted by other peers with the target peer, the credibility factor of these peers, and also the transaction context factor.

To compute the credibility factor, authors proposes two options. The first option is to use the existing trust values of the recommender peers which are stored in the requestor peer's repository. The second option is to collect the similarity credibility measure between the requestor peer and the recommender peers of a set of common providers, similar to Collaborative Filtering algorithm that is discussed in sub-section A. The authors argue that the second choice solves the issues of misleading feedbacks from the credible peers. The transaction context factor incorporates various transaction contexts (e.g. size, category, time-stamp, etc.) to better weight the recent and important transactions. The introduction of community factor provides an incentive or reward for the recommender peers to gives their feedback. In its implementation, each peer in PeerTrust model has a trust manager responsible for submitting and collecting the feedback as well as for performing the trust evaluation. In addition, each peer also has a database or repository to store the trust value. Based on the conducted experiment, authors found that the similarity based measures to calculate the credibility factor is more efficient than the peers' trust value weightage in both collusive and non-collusive settings.

F. Peer to Peer Multidimensional Trust Model

Authors in [40] propose a multidimensional trust models that encompasses several dimensions of trust values, such as users, knowledge, services or nodes, and social inter-institutional. In this multidimensional model, every entity keeps a list of opinions of other entities, data, services and nodes. A Distributed Knowledge Base (DKB) is utilized to search and update these lists. Each entity has a contact list which lists all trusted entities in a specific context and trust value. The trust value for an unknown entity is computed based on the reputation of that entity based on the trusting entity's contacts. In the list of opinions, each entity would keep his experiences with other entities. Each opinion consists of subject, object, keywords and value. Subject is an entity that provides the opinion about the object or target entity, keywords provide the contextual information about the opinion, and value contains the credibility value of this opinion. The trust rating is represented as probabilistic values ranges from 0 (no trust) to 1 (complete trust).

Similar to REGRET, this model allows the referral model in which a contact is able to retrieve the values of a target entity from other contacts. Further, in order to keep track of entity's actions in a system, this model uses the concept of Credential Provider (CP) that is commonly used in identity management. CP is used to authenticate the entities on each service provider and also to establishing trust relationship with another CPs. In an event where an entity uses the certificate from his Certificate Authority (CA), the trust value of this user is automatically computed based on CA's value in a particular CP. DKB is used to register the institutions and keep the meta-data certificate and social status of the institutions. Therefore, it can be inferred that this model is considered as centralized model where central servers provide the management of trust.

G. DEco Arch

DEco Arch [41] is trust and reputation service brokering architecture that is tailored for digital ecosystems [9]. DEco Arch addresses some issues faced by Universal Description, Discovery and Integration (UDDI) [42] as a central registry for service brokering, such as issue in central managed registry service, issue in non-transparent trustworthiness value and reputation rankings, etc. This model is applied on the semantic peer to peer architecture, such as JXTA [43], and it stores the trustworthiness, reputation values in Distributed Hash Database

(DHT) [44]. DEco Arch provides the service discovery by matching the semantic attribute of service consumers with the services or product descriptions in Resource Description Format (RDF) [45] format.

DEco Arch introduces the group alliance concept in which services are grouped together based on the semantic similarities. Each group alliance has the reputation value ranges from -1 (unknown), 0 (very bad reputation) to 5 (very good reputation). This reputation value is associated with the trend value (i.e. decreasing, neutral, and increasing) and the confidence value (0, 1) which depends on the number of contributing entities. The reputation value of a group alliance is computed as the weighted average of the aggregated reputation values of its members while the individual reputation value is computed based on the membership percentage. The inclusivity of a new service provider into a group alliance is decided based on its semantic matching degree and individual reputation value. The group alliance rejects the service provider whose reputation value is low as it would affect the reputation value of the alliance. Further, it put the unknown or new service provider in a sandbox until it gains better reputation value. In case of dishonest entity provides wrong opinion, authors argue that the credibility value of this entity is only included in the trustworthiness computation during selection process.

H. TRAVOS

TRAVOS [46] is a trust model that is proposed for managing trust in a multi-agents environment, such as Grid environment. It utilizes the probabilistic and beta distribution (bayesian) method to measure a probability that a provider agent will be trustworthy in fulfilling its obligation. TRAVOS measures trustworthiness of a provider agent based on 2 criteria: (i) consumer agent's past experience (direct interactions with the provider agent) and (ii) provider's reputation (ratings) that are perceived by other agents (raters). For the first criteria, TRAVOS utilizes *probability density function* (pdf) to model the probability of random variable in which pdf's beta family is used to measure the probability that a provider's agent will fulfill its obligation.

To compute the provider's reputation perceived by other agents, TRAVOS first estimates the accuracy (credibility) of the ratings based on all accurate and inaccurate advice provided by the raters in the past. The accuracy of ratings is measured through beta distributions similar to the computation of consumer's past experience. Once the accuracy of ratings is computed, it then adjusts these ratings according to their accuracy. TRAVOS only include the accurate ratings for its computation while discarding those inaccurate ratings. The approach that is taken by TRAVOS in measuring the accuracy of ratings differs significantly from other similar Bayesian approach in the literature, such as the Beta Reputation System (BRS) [47]. In BRS, agent's rating that differs significantly from the majority of ratings is deemed inaccurate and discarded from computation.

I. Measuring Trustworthiness using Personalized Approach

Authors in [48] proposed a personalized method for measuring the trustworthiness of sellers in e-marketplaces. Its trust model is classified as binary model that takes into account the buyer's past interactions with a seller and also the reputations of a seller. In addition, a novel approach for estimating the credibility of ratings provided by the raters is presented. Authors used two methods for measuring the credibility of ratings: (i) Private method: buyer estimates the reputation (credibility) of a rater based on the ratings on the same set of sellers, (ii) Public method: all ratings of the sellers that a rater has ever provided. In private method, buyer will retrieve all sellers' ratings that each rater has provided. Buyer then identifies a same set of sellers that he and the rater has rated. He then compares his ratings and the ratings provided by the rater on the same set of sellers and within a given context and time. Such comparison measures the credibility of the rater.

Public method is introduced to manage the unavailability of private knowledge that the buyer has with the rater (e.g. buyer never request ratings from the rater). Public method requires central servers to store all ratings provided by all raters in the environment. These central servers are responsible for measuring the credibility of raters by comparing the similarity measures between the ratings provided by each rater and the overall ratings provided by the majority of raters on a same set of sellers. Note that, as previously discussed, the centralized structure suffers from single point control and failure.

VII. Requirements for Trust Model in Digital Environments

In this section, we present several requirements for a trust model in digital environments. Considering all characteristics of digital environments discussed in section III, we derive a list of requirements for an appropriate trust model in digital environments:

1) *Distributed Model that finds other users that have consumed the similar service*: As trust through reputations is heavily relied on third-party (termed as raters) recommendations, there is a need for a user to identify other users (raters) that have consumed the particular services for the purpose of requesting the recommendations. However, finding raters is a challenging task as raters are mostly unknown to the users. Furthermore, digital environment requires a distributed model to limit the single point failure and control.
2) *Model that measures the relativeness perception of different users on the satisfaction levels of service provider*: The perception of each user on the satisfaction of provider's service varies. For example, a user may rate a provider's service as good although it collects user's information without consent. However, other users may rate the same service as bad.
3) *Model that identifies the dishonest raters in providing rating feedbacks*: It is highly possible that raters are malicious or dishonest in providing rating feedbacks. For example, a provider that offers service in digital environments may get his friends and families to give good rating to his service although it has low quality and

violates privacy. In this case, the legitimate users may be tricked to believe that such service is good and therefore, they consume it.

4) *Model that mitigates several threat strategies that subverting rating system*: Literature has presented a number of threat strategies that are used to subvert trust system [24, 26]. One of the most severe threat strategies is providers engage in a collaborative agreement to provide good ratings to each other services while give other services bad ratings.
5) *Model that provides incentives to rate*: Another challenge in building a successful reputation trust system is in providing the incentives for users to give their rating feedbacks.

VIII. Conclusion

The main functionalities of digital environments are to allow entities to share their resources, information, knowledge, services, etc. and also to enable transactions between entities in open, heterogeneous and dynamic environments. However, the successful of digital environments in achieving these functionalities can only be realized if its member entities are able to trust each other. To ensure trust relationship is nurtured, there must be a framework to determine, measure, and compute the trustworthiness value of any entity in the environment. Further, this framework must also encourage entities' involvement to provide their recommendations to others. Developing an effective trust framework has proven to be difficult. This is due to the multi-faceted concept of trust that encompasses the four main elements: belief, reputation, context, and time. Furthermore, the requirement of highly performing digital environments that encourage de-centralised approach gives additional challenge in developing an effective trust framework.

This paper firstly provided an overview of digital environments. The evolution of digital environment over the years has been presented. In addition, the paper also presented the forthcoming state of digital environments and their important characteristics. The discussion followed through with an extensive review of the notion and characteristics of trust. In addition, the four important elements of trust were also presented in this paper. Next, this paper provides overview of several existing trust models from the literature. Each of these trust models has been detailed in the paper. Lastly, the requirements for an appropriate trust models in digital environments were discussed. These requirements play a pivotal role for deriving an appropriate trust model for digital environments. Future work includes proposing a trust model for digital environments that meets the identified requirements.

References

[1] T. Grandison and M. Sloman. (2000). A Survey of Trust in Internet Applications [IEEE Communications Surveys and Tutorials, Fourth Quarter]. Available: http://www.comsoc.org/pubs/surveys/

[2] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provisioning," Decision Support System, vol. 43, pp. 618-644, 2007.

[3] E. Grandon and J. Pearson, "Electronic commerce adoption: an empirical study of small and medium US businesses," Information and Management, vol. 42, pp. 197-216, 2004.

[4] F. Nachira, E. Chiozza, H. Ihonen, M. Manzoni, and F. Cunningham, "Towards a network of digital business ecosystems fostering the local development," Bruxelles, Report, 2002.

[5] D. F. Ross, Introduction to Supply Chain Management Technologies, 2nd ed.: CRC Press, 2010.

[6] J. L. Lipnack and J. S. Stamps, The Age of the Network. New York: John Wiley & Sons, 1994.

[7] H. Boley and E. Chang, "Digital Ecosystem: Principles and Semantics," presented at the 2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2007), Cairns, Australia, 2007.

[8] F. Nachira, P. Dini, and A. Nicolai. (2007, 14 September 2011). A network of digital business ecosystems for Europe: roots, processes and perspectives. Introductory Paper [Introductory Paper]. Available: http://www.digital-ecosystems.org/book/DBE-2007.pdf

[9] G. Briscoe and P. Wilde, "Digital Ecosystems: Evolving Service-Oriented Architectures," in Proceedings of the 1st international conference on Bio inspired models of network, information and computing systems, New York, USA, 2006.

[10] A. L. Blanchard and L. Markus, "The Experienced "Sense" of a Virtual Community: Characteristics and Processes," *ACM SIGMIS Database,* vol. 35, pp. 65-79, 2004.

[11] F. T. Rothaermel and S. Sugiyama, "Virtual internet communities and commercial success: individual and community-level theory grounded in the atypical case of TimeZone.com," *Journal of Management,* vol. 27, pp. 297-312, 2001.

[12] S. Benford, C. Greenhalgh, T. Rodden, and J. Pycock, "Collaborative Virtual Environments," *Communications of The ACM,* vol. 44, 2001.

[13] E. F. Churchill, D. N. Snowdon, and A. J. Munro, Collaborative Virtual Environments: Digital Places and Spaces for Interaction. London: Springer-Verlag, 2001.

[14] M. Deutsch, Distributive justice: A social psychological perspective. USA: Yale University Press, 1985.

[15] N. Luhmann, "Familiarity, Confidence, Trust: Problems and Alternatives," in In Trust: Making and Breaking Cooperative Relations, ed New York, USA: Basil Blackwell Publisher, pp. 94-107.

[16] J. Dunn, The Concept of Trust in the Politics of John Locke. Cambridge, UK: Cambridge University Press, 1984.

[17] D. Gambetta. (2000, Can we trust trust? Trust: Making and Breaking Cooperative Relations [electronic edition]. Available: http://www.sociology.ox.ac.uk/papers/gambetta213-237.pdf

[18] C. Castelfranchi and R. Falcone, "Principles of Trust for MAS: Cognitive Anatomy, Social Importance, and Quantification," in Third IEEE International Conference on Multi-Agent Systems, Los Alamitos, 1998.

[19] Entrust. (2000, April 2011). The concept of trust in network security, Version 1.2 [White Paper]. Available: Http://www.entrust.com/resources/pdf/trust.pdf

[20] J. Ghosen. (2002, May 2011). Study Shows Perceived Risk of Online Credit Purchase Linked to Trust, Familiarity with Intermediaries. Available: http://www.buffalo.edu/news/fast-execute.cgi/article-page.html?article=59430009

[21] C. Liu and M. A. Ozols, "Trust in secure communication systems—The concept, representations, and reasoning techniques," in Proceedings of the 15th Australian Joint Conference on Artificial Intelligence: Advances in Artificial Intelligence, Canberra, Australia, 2002.

[22] F. K. Hussain and E. Chang, "An Overview of the Interpretations of trust and reputation," presented at the The Third Advanced International Conference on Telecommunications (AICT 07), Mauritius, 2007.

[23] E. Chang, F. K. Hussain, and T. S. Dillon, "Fuzzy nature of trust and dynamic trust modelling in service oriented environments," presented at the 2005 workshop on secure web services, Fairfax, VA, USA, 2005.

[24] E. Chang, T. Dillon, and F. K. Hussain, Trust Reputation for Service-Oriented Environments. West Sussex, England: John Wiley & Sons Ltd, 2006.

[25] A. Josang, "The Right Type of Trust for Distributed Systems," in Proceedings of the 1996 workshop on new security paradigms, Lake Arrowhead, USA, 1996.

[26] A. Abdul-Rahman and S. Hailes, "Supporting trust in virtual communities," in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Hawaii, USA, 2000.

[27] L. Mui, M. Mohtashemi, and A. Halberstadt, "Notions of reputation in multi-agents systems: a review," in Proceedings of the 35th Hawaii International Conference on System Sciences, Big Island, USA, 2002.

[28] L. Mui, M. Mohtashemi, and A. Halberstadt, "Evaluating Reputation in Multi-agents Systems," in Proceedings of the International Workshop on Trust, Reputation, and Security: Theories and Practice, Bologna, Italy, 2002.

[29] eBay.com. (June 2011). eBay Website. Available: http://www.ebay.com/

[30] Amazon.com. (June 2011). Amazon Website. Available: http://www.amazon.com/

[31] B. Yu and M. P. Singh, "An Evidential Model of Distributed Reputation Management," in Proceedings of the first international joint conference on Autonomous agents and multiagent systems, Bologna, Spain, 2002.

[32] B. Yu and M. P. Singh, "A Social Mechanism of Reputation Management in Electronic Communities," in Proceedings of the 4th International Workshop on Cooperative Information Agents IV, The Future of Information Agents in Cyberspace, Boston, USA, 2000.

[33] D. Goldberg, D. Nichols, B. M. Oki, and D. Terry, "Using collaborative fltering to weave an information tapestry," Communications of the ACM, vol. 35, pp. 61-70, 1992.

[34] Z. Noorian, S. Marsh, and M. Fleming, "Multi-Layer cognitived filtering by behavioural modelling," in In Proceedings of the 10th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2011), , Taipei, Taiwan., 2011.

[35] J. Sabater and C. Sierra, "REGRET: A reputation model for gregarious societies," in Proceedings of the fifth international conference on Autonomous agents, Montreal, Canada, 2001.

[36] A. Singh and L. Liu, "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems," presented at the Third International Conference on Peer-to-Peer Computing, Sweden, 2003.

[37] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," presented at the presented at the 12th ACM international conference on World Wide Web, USA, 2003.

[38] L. Page, S. Brin, R. Motwani, and T. Andwinograd, "The PageRank citation ranking: Bringing order to the Web," Stanford University, Technical Report, Stanford, CA, 1998.

[39] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," IEEE Transactions on Knowledge and Data Engineering, vol. 16, pp. 843-857, 2004.

[40] M. Ion, A. Danzi, H. Koshutanski, and L. Telesca, "A Peer-to-Peer Multidimensional Trust Model for Digital Ecosystems," presented at the Second IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2008), Phitsanulok, Thailand, 2008.

[41] S. Schmidt, R. Steele, and T. Dillon, "DEco Arch: Trust and Reputation Aware Service Brokering Architecture in Digital Ecosystems," presented at the Inaugural IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST), Cairns, Australia, 2007.

[42] T. Bellwood. (2002, May 2011). Understanding UDDI. Available: http://www.ibm.com/developerworks/webservices/library/ws-featuddi/

[43] L. Gong. (2001) JXTA: a network programming environment. IEEE Internet Computing. 88-89.

[44] S. Rhea, et al., "OpenDHT: a public DHT service and its uses," in Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications., Philadelphia, Pennsylvnia, USA, 2005.

[45] W3C. (May 2011). Resource Description Framework (RDF). Available: http://www.w3.org/RDF/

[46] W. T. L. Teacy, J. Patel, N. R. Jennings, and M. Luck, "Travos: Trust and reputation in the context of inaccurate information sources.," Journal of Autonomous Agents and Multi-Agent Systems, vol. 12, 2006.

[47] A. Josang and R. Ismail, "The Beta Reputation System," in in Proceedings of the 15th Bled Electronic Commerce Conference, 2002.

[48] J. Zhang and R. Cohen, "Evaluating the trustworthiness of advice about seller agents in e-marketplaces: A personalized approach," Elsevier Journal of Electronic Commerce Research and Applications, vol. 7, pp. 330-340, 2008.