IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON TRENDS AND ADVANCES FOR AMBIENT INTELLIGENCE WITH INTERNET OF THINGS (IOT) SYSTEMS

Received February 10, 2017, accepted February 28, 2017, date of publication March 3, 2017, date of current version April 24, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2677917

Event-Driven Trust Refreshment on Ambient Services

HOANG LONG NGUYEN[1], O-JOUN LEE[1], JAI E. JUNG[1], JAEHWA PARK[1], TAI-WON UM[2], AND HYUN-WOO LEE[2]

[1]Department of Computer Science and Engineering, Chung-Ang University, Seoul 06911, South Korea
[2]Hyper-connected Communication Research Laboratory, Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea

Corresponding author: J. E. Jung (j3ung@cau.ac.kr)

This work was supported in part by the ICT R&D Program of MSIP/IITP, Development of TII (Trusted Information Infrastructure) S/W Framework for Realizing Trustworthy IoT Eco-system under Grant R0190-15-2027 and in part by the Business for Cooperative R&D between Industry, Academy, and Research Institute through the Korea Small and Medium Business Administration in 2016 under Grant C0443994.

ABSTRACT Since trust among entities can change according to various conditions, it is necessary for ambient services to determine when and how the trust has to be updated. Therefore, our contribution in this paper is to present: 1) a new definition of trust that can be extended to various domains; 2) a novel method based on social events and patterns to trigger trust refreshment in ambient services; and 3) a web application framework (called SocioScope) for collecting and analyzing data from multiple data sources. Finally, the case study suggests that this proposal could be applied to trust-aware ambient and recommendation systems.

INDEX TERMS Trust, trust refreshment, social event, complex event, ambient service.

I. INTRODUCTION

Trust is an essential factor in human interaction. Therefore due to its importance, it has been of interest in many research efforts in many diverse areas (e.g., philosophy, psychology, society, or even natural science). In our daily life, almost all conventional activities (e.g., believing in a thing, or making the decision to purchase a product) contain uncertainty. Therefore, trust is a key element to guide human action. In short, it is one of the crucial factors that affect human behavior. Trust widely exists in our life, even though we may not be aware of it.

A large number of studies focus on proposing the definition of trust as sociological concept [1]–[3], philosophical perspective [4], [5], psychological point of view [6], [7], or computational concept [8]. In particular, Rotter [9] defines interpersonal trust as a generalized expectancy. Golbeck [10] determines trust as a commitment to an action with the belief that the trustee will act in the right way to obtain a good outcome in the future. Reference [11] mentions trust as the composition of belief properties (i.e., competence, disposition, dependence and fulfillment). However, these definitions are domain-specific, and still complex. Hence, we aim to propose a general and simple definition of trust. This definition can be extended to different domains with various types of entity. We then build a trust ontology, which is helpful for intelligibly expressing our trust definition.

In addition, other research concentrates on solving the problem of modeling and representing trust by using ontology-based approaches [12]–[15], or network-based methods [16]–[18]. The survey in [19] showed that studies related to trust could be applied to various areas, such as security [20]–[22]; web of trust [23]–[25]; game theory and agents [26], [27]; and semantic web [28], [29].

However, a limitation to this research is the change in Trust. Our beliefs are not static, nor rigid. When more information becomes available, our trust is refreshed. Thus, we need to update our beliefs. When we were children, we were told what is the right thing to do, and we acted on instinct. By growing, we obtain more knowledge from learning. Gradually, we change our mind, and get to decide what we want to believe. We are now living in the time of big data, which is effortlessly generated with the support of the Internet of Thing (IoT) technologies (e.g., smart mobile devices, sensors, trackers). As reports, each minute we send around 200 million emails, post almost 300,000 tweets, and upload about 300,000 photos to Facebook. These data implicitly contain social events (the definition of ''event'' is later explained in Sec. III). This is a major rationale that affects our belief.

For example, we may have confidence in a phone model when it is first launched. Later, an event of battery explosion of this phone occurs. This could likely decrease our trust toward this product. Understanding trust updating is really helpful in recommendation systems [30]–[32].

To express the trust refreshment, we propose five types of pattern, which are stable, abrupt, incremental, gradual, and reoccurring patterns. Every time an event occurs, the trust is recalculated. Using the degree of trust by time, we could decide the type of pattern that our trust refreshment belongs to. There are many advantages to be gained from understanding the change of trust (e.g., promptly adjusting advertisement strategies when the trust of people in a product is decreased).

This paper is organized as follows. This section has provided a short introduction to our work in this paper. Section II describes in detail the definition of trust and different patterns of trust refreshment. Next, Sec. III proposes an explanation for IoT-based social events. Section IV presents a case study to further demonstrate the efficiency of our work. Finally, Sec. V concludes the paper, and suggests some future works.

II. UNDERSTANDING TRUST

In this section, our purpose is to propose a general definition of trust that could be extended to various domains. Also, we compose an ontology of trust for giving an overview perspective of our definition. Finally, we introduce and define patterns of trust refreshment with the use of trust definition.

A. DEFINITION OF TRUST

We define trust among every kind of entity in a domain. Also, to apply this definition to ambient services and the IoT environment, we should reduce its domain-dependency. Therefore we make the following assumption:

Assumption 1: A thing is trusted when we hope that it will perform as we expect. For example, we trust a phone, if we expect that it will work normally without any problem.

We realize that sometimes there is ambiguity between definitions of trust and reputation. Furthermore, some works mentioned that trust and reputation share the same meaning. Nevertheless, trust is our prediction about the future, while reputation represents the fame of an entity, due to its achievements in the past. We emphasize that reputation could build trust, but it is not equivalent to trust. An entity with high reputation does not ensure that it must get high beliefs from other entities.

Definition 1 (Trust): Based on our assumption, we simply define trust as expectation. Eq. 1 is a formulation of trust, which is the quadruple of

$$\mathcal{T} \equiv \{\Upsilon, \Sigma, \mathcal{C}, \mathcal{D}\} \tag{1}$$

where $\mathcal{T}$ is trust, Υ is a trustor, Σ is a trustee, $\mathcal{C}$ is a context, and $\mathcal{D}$ is a degree of trust (DoT). Elements of $\mathcal{T}$ can be defined as below, respectively.

In this work, we suppose that all the entities in a domain can be trustors or trustees. Also, among trustors and trustees, social or functional relationships exist; we term them linkages. Forms and types of linkages are determined, depending on the domains and kinds of entities that are on each end of the linkage. For example, the relationships between a chef and his or her customers can be simplified as producer−consumer. When the customers are the trustors, a degree of trust among them is decided from the quality of food, right price, cleanliness of the kitchen, and so on. On the other hand, when the chef is a trustor, the degree of trust might be determined based on the honesty of the customers reviews, and so on. Based on this, we define trustor and trustee as follows:

Definition 2 (Trustor): Trustor could be comprehended as "grantor". It is the entity that is the source of trust. In our definition, an entity is an abstract term that includes every kind of actor in an applied domain. Depending on a particular scenario, a trustor could be a person, a device, a service, or so on.

Definition 3 (Trustee): The trustee is an entity that obtains the trust from a trustor. Similar to trustor, a trustee could be a person, device, or other kind of entity. The social or functional relationship between trustor and trustee is a linkage.

The trust between trustor and trustees is not a constant parameter. It keeps changing, depending on alterations of the contexts. For example, a person A could believe in another person B, based on their experience in selecting dishes when they are at a restaurant. However, in other circumstances (e.g., buying or fixing machines), it is uncertain whether A might trust B, or not. Accordingly, we define context as follows:

Definition 4 (Context): Context is a situation that affects the trust between trustor and trustee. The context between the trustor Υ and trustee Σ can be formulated as:

$$\mathcal{C}(\Upsilon, \Sigma) \equiv \{\mathcal{T}, \mathcal{L}, \Theta\}, \tag{2}$$

where $\mathcal{T}$ is a certain topic, $\mathcal{L}$ is a specific location, and Θ is a particular time point.

The topic, location, and time point of the context indicate what the context is related to, where it happened, and when it happened, respectively. The topic is used to decide conformity of the context with the trustors and trustees, since not every event that happens in the same domain is relevant to their trust. For example, avian influenza may be an issue for a domain restaurant business; however, it will not critically affect BBQ restaurants. In other cases, they also used to decide temporal/spatial relevancy, similar to the topic.

There are many measurements to estimate the degree of trust. Its value could be expressed by using a number of levels [33], or continuous numbers within a particular range [34], [35]. However, fuzzy number is the most suitable option for measuring DoT, since it enables the reduction of domain-dependency and can be applied for various algorithms, systems, and applications. Therefore, we newly define the degree of trust as follows:

Definition 5 (Degree of Trust): The degree of trust indicates how much trustor Υ trusts trustee Σ. Based on the fuzzy concept, we represent the degree of trust as a real number that

belongs to the range $\mathbb{Z} \in [0, 1]$.

$$\mathcal{D} : \Upsilon, \Sigma \mapsto x \ \ with \ \ x \in \mathbb{Z}, x \in [0, 1] \tag{3}$$

where x is DoT between Trustor Υ *and Trustee* Σ.

Conclusively, trust $\mathcal{T}$ is a weighted-directed edge that has a source (trustor Υ), and a destination (trustee Σ). Also, it is not represented as boolean value or discrete number, but as a fuzzy number $\mathcal{D}$, which is continuous, normalized, and of convex numerical value. The degree depends on the environmental context $\mathcal{C}$.

B. TRUST ONTOLOGY

To regularize elements of trust and their relations, we use ontology as a powerful tool to represent the semantic of our trust definition above. This is helpful for not only human, but also machine processing. To maximize the advantages of using the ontology, it should be general and flexible to be easily applied to various domains. However, most of the existing trust ontologies are domain-specific [12], [13], [15].

As mentioned before, we define the trust between entities, not among only users, or from users to entities. Defining the trust only for users, agents, or objects is relatively easy. Nevertheless, since our definition includes every kind of entity, and the entities can be both trustors and trustees, we should make a comprehensive definition for them. Therefore, we minimize the attributes of our ontological model for trust as in Fig. 1, which is composed by consolidating former research, particularly that based on Ceolin *et al.* [15] and Viljanen [13].

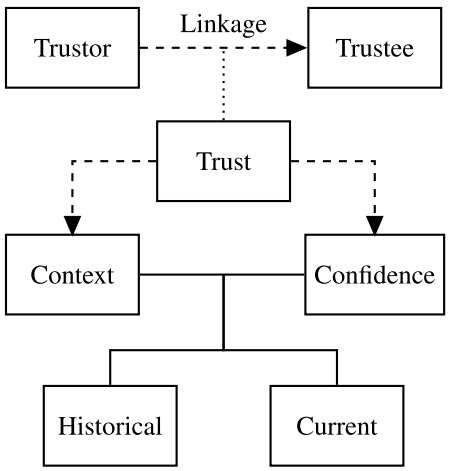

FIGURE 1. The Trust Ontology.

Figure 1 shows that ontological model of trust mainly focuses on context-awareness and temporal dynamicity of trust. It is based on the simple relation of ''Trustor'' and ''Trustee'', which terms are already defined in [13]. This relation is extended based on social relations between them with considering their ''Trust''. The trust is decided based on their ''Context'' and ''Confidence''. When we determine Trust, historical changes of ''Context'' and ''Confidence'' are also considered, not only the current state. The attributes of trust are emphasized in detail as follows:

- Linkage: Linkage is a relationship between two arbitrary entities. It is different from the type of each entity. If two entities are both users, the linkage between them could be a social relationship, or a social affinity. Otherwise, one entity is a content delivery platform, while the other is its user, and their linkage might be provider−consumer. The linkages are categorically described.
- Context: Context means the environmental conditions of entities, particularly those that can affect the entities degree of trust. This is applied to reflect ambient states for measuring the trust. Also, it is considered not only as a current state, but also the historical changes of state.
- Confidence: Confidence is another notion of DoT. This indicates the certainty of a trust. In other words, it means how much we can believe the degree of trust for the relation. It is used as a weighting value for propagating trusts, and aggregating the results of the propagation. As with the context, it is considered as both current and historical certainties.

With the use of trust definition, we only understand its semantic at a particular circumstance. Therefore, our major focus is to define another theory to present dynamic changes, and those of trust according to time. Measuring the trust between entities is beyond our coverage.

C. TRUST REFRESHMENT

To understand the change of trust, we clarify and categorize patterns of trust refreshment in this section. By applying the theory of concept drift [36]–[38], we categorize the changes of trust into 4 types of pattern, which are abrupt, incremental, gradual, and reoccurring patterns. In addition, we propose a novel type of trust transformation, which is stable pattern. Despite the relationship between trustor and trustees being obviously a one-to-many correspondence, for the sake of simplicity we restrict the number of trustees in this study to be within $\mathbb{N} \in [1, 2]$. Before going into detailed explanation, we would like to identify some major notions, as follows:

- For convenience in mathematical expressions, the DoT of trustor Υ to trustee Σ_A (i.e., $\mathcal{D}(\Upsilon, \Sigma_A)$) is abbreviated as $\mathcal{D}_A$.
- The DoT of trustor Υ to trustee Σ_A and to trustee Σ_B are complementary to each other.

$$\mathcal{D}_B = \overline{\mathcal{D}_A} = 1 - \mathcal{D}_A \tag{4}$$

- We use t_i and t_j to discuss the starting time point and ending time point of a pattern. In addition, t_k is the mid-point between t_i and t_j in which the trust update happens.
- We only use the DoT between trustor Υ and trustee Σ_A for mathematical expressions. The DoT for trustee Σ_B can be expressed in the same way as for trustee Σ_A.

Definition 6 (Stable Pattern): Stable pattern is a fundamental type of trust refreshment. It means that the DoT of

trustor Υ *has not been changed over time. This can be formulated as:*

$$\mathcal{P}(\Upsilon, [t_i, t_j]) = \mathscr{S} \ \ if \ \ \mathcal{D}_A^{t_i} \cong \mathcal{D}_A^{t_j}, \tag{5}$$

where $\mathcal{P}(\Upsilon, [t_i, t_j])$ *is the trust refreshment pattern of trustor* Υ *in a time interval* $[t_i, t_j]$.
Figure 2 shows the stable pattern.

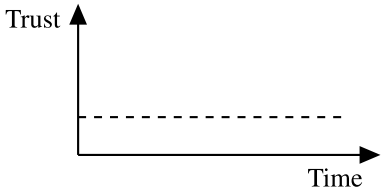

FIGURE 2. The Stable Pattern.

Definition 7 (Abrupt Pattern): Abrupt pattern is used to present a complete alteration of a belief of trustor Υ *from trustee* Σ_A *to trustee* Σ_B*, and vice versa. It can be expressed as*

$$\mathcal{P}(\Upsilon, [t_i, t_j]) = \mathscr{A} \ \ if \ \ \begin{cases} |\mathcal{D}_A^{t_k} - \mathcal{D}_A^{t_{k+1}}| = 1, \exists t_k \\ \mathcal{D}_A^{t_i} = \mathcal{D}_A^{t_k}, \mathcal{D}_A^{t_{k+1}} = \mathcal{D}_A^{t_j}. \end{cases} \tag{6}$$

Figure 3 shows abrupt pattern.

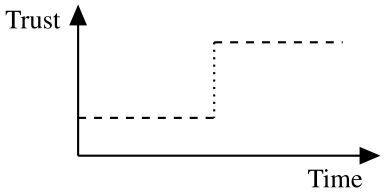

FIGURE 3. The Abrupt Pattern.

Definition 8 (Incremental Pattern): In the case of incremental pattern, the trustor Υ *incrementally changes their belief from trustee* Σ_A *to trustee* Σ_B *according to time, and vice versa. With incremental pattern, trustor* Υ *might trust trustee* Σ_A *and trustee* Σ_B *at the same time with different DoT values. This can be formulated as:*

$$\mathcal{P}(\Upsilon, [t_i, t_j]) = \mathscr{I} \ \ if \ \ \mathcal{D}_A^{t_k} - \mathcal{D}_A^{t_{k+1}} > 0, \forall t_k. \tag{7}$$

Incremental pattern can be depicted as Fig. 4.

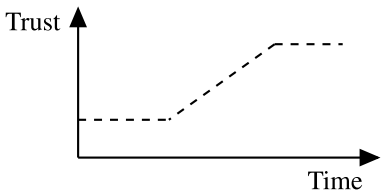

FIGURE 4. The Incremental Pattern.

Definition 9 (Gradual Pattern): Similar to the incremental pattern, gradual pattern is also used to show the changes of trust step-by-step during a time interval. However, different from the incremental pattern, the gradual pattern means that trustor Υ *only trusts trustee* Σ_A *or trustee* Σ_B *at a particular time point. This can be expressed as:*

$$\mathcal{P}(\Upsilon, [t_i, t_j]) = \mathscr{G} = \{\mathscr{A}^{t_a, t_b} \mid t_i < t_a < t_b < t_j\}, \tag{8}$$
$$if \ |\mathscr{A}^{t_a, t_b}| > 2, |\mathcal{D}_A^{t_i} - \mathcal{D}_A^{t_j}| = 1.$$

Figure 5 shows gradual pattern.

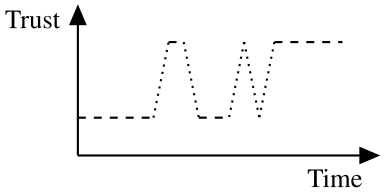

FIGURE 5. The Gradual Pattern.

Definition 10 (Reoccurring Pattern): The reoccurring pattern is an extension of abrupt pattern. It indicates the case that a trusted trustee is the same at the starting point and the ending point, in spite of the changes of DoT within the time interval.

$$\mathcal{P}(\Upsilon, [t_i, t_j]) = \mathscr{R} = \{\mathscr{A}^{t_a, t_b} \mid t_i < t_a < t_b < t_j\} \tag{9}$$
$$if \ |\mathscr{A}^{t_a, t_b}| = 2, |\mathcal{D}_A^{t_i} - \mathcal{D}_A^{t_j}| = 0$$

The reoccurring pattern can be depicted as Fig. 6.

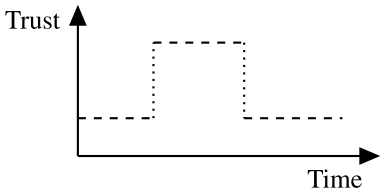

FIGURE 6. The Reoccurring Pattern.

If there is an update of our trust, it will belong to one of the above patterns. In the next section, we aim to propose a circumstance in which we need to refresh our trust.

III. EVENT-DRIVEN TRUST REFRESHMENT

Although we have known about what is trust and how to estimate the DoT, we have to discover when the appropriate time point is for analyzing the trust. Most of the existing works have not considered dynamicity of trust according to changes of the context. Even though they have taken into account the context, it mainly has been focused on social relationships between entities.

With an advent of IoT paradigm, data sources are moving to smart devices such as trackers, sensors, or smart IoT systems. It makes the amount of information and data which computer systems need to handle is rapidly increased. Also, it causes us to have to face with a large amount of information everyday in our life. Although our trust is a dynamic concept, it is not transformed without any reason. Due to our study, social event is an important reason which cause the change of trust because it contains the herb behavior property. We would like to propose the definition of social event before entering into a real case study.

We obtain the definition from [39] and [40] with two types of events:

- Complex event: contains the set of single events that are related to a unique topic

$$\mathcal{E}(\mathcal{T}) = \bigcup_{i=1}^{n} e_i = \{e_1, e_2, \ldots, e_n \mid e_i \in \mathcal{T}\} \quad (10)$$

  where $\mathcal{E}$ is a complex event, and T is the topic of a complex event that the single events belong to.
- Single event: is an abnormal phenomenon in a collection of data. A single event describes a topic that occurs in a certain location at a particular time

$$e = \{\mathcal{T}, \mathcal{L}, \Theta\} \quad (11)$$

  where $\mathcal{T}$ is the topic, $\mathcal{L}$ is the location, and Θ is the time point when the single event happens.

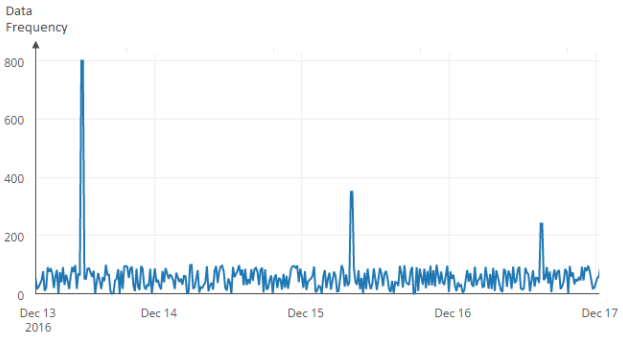

FIGURE 7. Single events that are related to the complex event "Thank You Tour" of Donald Trump in 2016.

For example, Fig. 7 presents the information related to the complex event "Thank You Tour 2016" of President Donald Trump. In the complex event, there is a set of single events that are tours of different states (e.g., December 13 at West Allis, Wisconsin; December 15 at Hershey, Pennsylvania; and December 16 at Orlando, Florida).

Every time a single event happens, we need to update our trust. The set of DoT at every single event could produce a pattern pattern of trust refreshment. In next section, we demonstrate this idea with the use of SocioScope as our case study.

IV. SocioScope: A CASE STUDY FOR REPRESENTING TRUST REFRESHMENT

To conduct the experiment, we build a social data analysis framework, which is called SocioScope. Figure 8 shows the interface of SocioScope. The framework contains 2 major functions, which are: *i*) collecting data from multiple sources in IoT environments (e.g., sensors, smart devices, and social networking services [41]) that are related to a particular topic, and *ii*) providing tools for analyzing data (e.g., part-of-speech tagging, named entity recognition, sentiment analysis, and event detection). In this paper, we only focus on the event detection function, since this is the factor that affects

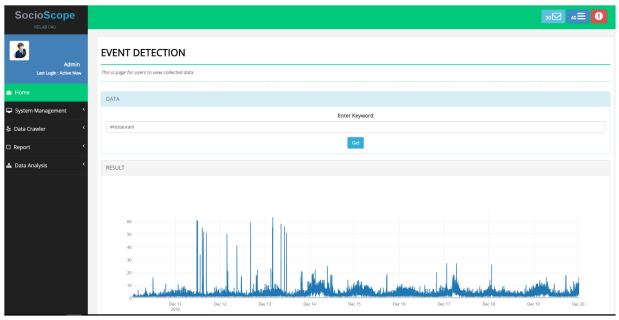

FIGURE 8. An interface of the SocioScope system.

the changes of trust. We explained this concept in detail in Sec. III.

We selected the 2016 US presidential election as the case study, which contains relatively specific "trustees". Also, we collected all the possible data for this election from many data sources (e.g., social networking services, trackers, and smart devices). In our scenario, the complex event is the 2016 US presidential election. Furthermore, the data was processed by using our SocioScope system to detect single events. After analyzing the time points of identified single events, we matched the temporal/spatial locations of the *i*) single events, and *ii*) announcements of US states of voting results, because people usually engage in social activities to share their emotion (e.g., posting social content through social networking services, calling or sending messages to other people) every time a voting result is announced. These actions implicitly create the single events.

Applying the definition of Trust in Sec. II to this situation, we determined trustor Υ as a user. Also, we limited the trustees to the two major candidates, Donald Trump (Σ_{Trump}) and Hillary Clinton ($\Sigma_{Clinton}$). The context is a single event that was discovered by our system. Measuring the DoT on initial states is beyond our coverage. We made the assumption that we already know how to calculate the degree of trust. Hence, we focused in this section on expressing patterns of trust refreshment. Figure 9 assumes that trustor Υ totally believes that Hillary Clinton will win the 2016 US presidential election. However, the voting result from each US state affects this users belief by time. We use circle graphs to represent the election results. We are able to easily realize that Donald Trump gets a higher proportion of votes by time. Therefore, the DoT of this trustor Υ to Hillary Clinton gradually decreases. Figure 9 shows that the trust refreshment pattern $\mathcal{P}$ of this user is of the incremental type.

Our trust needs to be updated according to time, since the trust has dynamicity. Therefore, it is very important to discover when and how we should re-estimate the trust among entities. Many advantages could be gained by understanding the proposed concept of trust refreshment. Returning to the case study, Hillary Clinton could have made prompt changes to improve her result, if she had known that the belief of the American people in her was decreasing. In other scenarios, companies could develop appropriate business strategies according to the trust of customers in their products. Also,

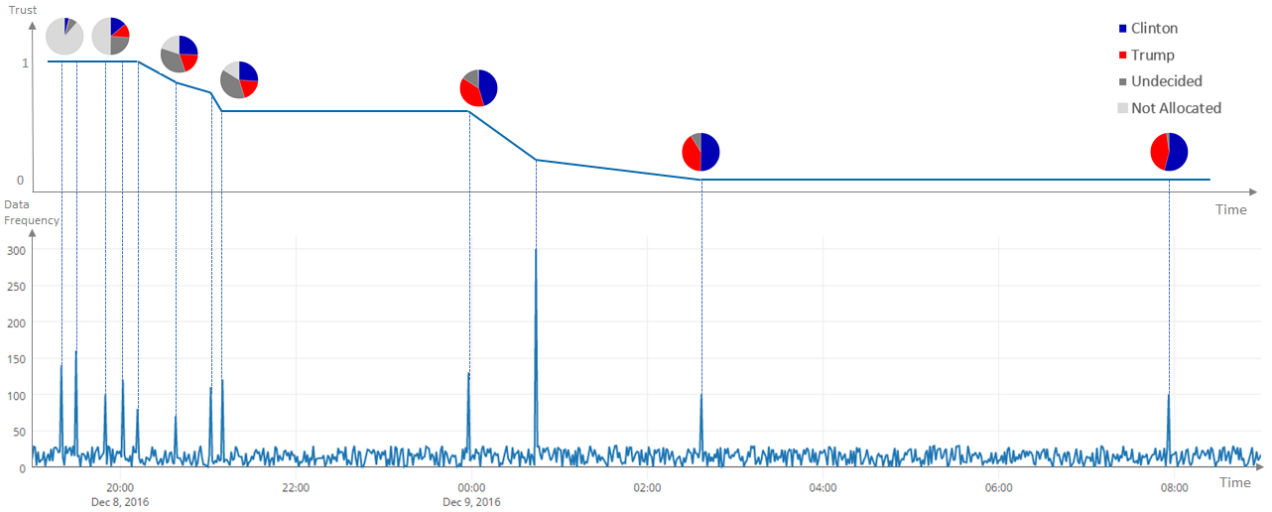

FIGURE 9. Trust refreshment of a user toward Clinton in the 2016 US presidential election.

security systems could recognize unsafe signals early, by detecting that the belief of data is decreasing.

V. CONCLUSION AND FUTURE WORK

In this paper, we propose a general and simple definition of trust. This definition could be extended to different areas. In order to more fully understand our definition, we build a simple ontology for visually expressing its meaning. In addition, our trust is a dynamic concept. Hence, we need to comprehend when and how our trust is refreshed. Our study shows that a single event is a time point that can affect the belief in an entity. To understand how trust changes, we propose five different types of pattern to represent trust refreshment (i.e., stable, abrupt, incremental, gradual, and reoccurring patterns). We demonstrate the effectiveness of our approach by using the SocioScope, which is a web application framework for collecting and analyzing data from multiple sources. We use the 2016 US presidential election in this paper as our case study.

We also state some future works. In the next research, we intend to comprehensively conduct more researches on extending the number of trustors Υ and trustees Σ to more than two entities in representing the patterns of trust refreshment. Next, methods for automatically discovering trust refreshment patterns will be integrated into the SocioScope system. Last but not least, other contexts in which trust could be updated will be considered as the most essential work.

REFERENCES

[1] B. Holzner, "Sociological reflections on trust," *Humanitas*, vol. 9, no. 3, pp. 333–345, 1973.

[2] J. D. Lewis and A. Weigert, "Trust as a social reality," *Social forces*, vol. 63, no. 4, pp. 967–985, 1985.

[3] P. Sztompka, *Trust: A Sociological Theory*. Cambridge, U.K.: Cambridge Univ. Press, 1999.

[4] N. Luhmann, "Trust and power," *Studies Soviet Thought*, vol. 23, no. 3, pp. 266–270, 1982.

[5] B. Williams *et al.*, *Trust: Making and Breaking Cooperative Relations*, 1st ed., D. Gambetta, Ed. Blackwell, Apr. 1988.

[6] R. M. Kramer and T. R. Tyler, *Trust in Organizations: Frontiers of Theory and Research*. Thousand Oaks, CA, USA: SAGE, 1995.

[7] R. B. Shaw, *Trust Balance: Building Successful Organizations Results, Integrity, Concern*. San Francisco, CA, USA: Jossey-Bass, 1997.

[8] S. P. Marsh, "Formalising trust as a computational concept," Ph.D. dissertation, Dept. Comput. Sci. Math., Univ. Stirling, Apr. 1994.

[9] J. B. Rotter, "A new scale for the measurement of interpersonal trust," *J. Pers.*, vol. 35, no. 4, pp. 651–665, Dec. 1967.

[10] J. Golbeck, "Computing with trust: Definition, properties, and algorithms," in *Proc. 2nd Int. Conf. Secur. Privacy Commun. Netw. Workshops (SecureComm)*, Baltimore, MD, USA, Aug./Sep. 2006, pp. 1–7.

[11] C. Castelfranchi and R. Falcone, "Principles of trust for MAS: Cognitive anatomy, social importance, and quantification," in *Proc. 3rd Int. Conf. Multiagent Syst. (ICMAS)*, Paris, France, Jul. 1998, pp. 72–79.

[12] J. Huang and M. S. Fox, "An ontology of trust: Formal semantics and transitivity," in *Proc. 8th Int. Conf. Electron. Commerce, New e-Commerce-Innov. Conquering Current Barriers, Obstacles Limitations Conducting Successful Bus. Internet (ICEC)*, Fredericton, NB, Canada, Aug. 2006, pp. 259–270.

[13] L. Viljanen, "Towards an ontology of trust," in *Proc. 2nd Int. Conf. Trust, Privacy Secur. Digit. Bus. (TrustBus)*, Copenhagen, Denmark, Aug. 2005, pp. 175–184.

[14] W. Sherchan, S. Nepal, J. Hunklinger, and A. Bouguettaya, "A trust ontology for semantic services," in *Proc. 7th IEEE Int. Conf. Services Comput. (SCC)*, Miami, FL, USA, Jul. 2010, pp. 313–320.

[15] D. Ceolin, A. Nottamkandath, W. Fokkink, and V. Maccatrozzo, "Towards the definition of an ontology for trust in (Web) data," in *Proc. 10th Int. Workshop Uncertainty Reasoning Semantic Web (URSW)*, Riva del Garda, Italy, Oct. 2014, pp. 73–78.

[16] J. Golbeck, B. Parsia, and J. Hendler, "Trust networks on the semantic Web," in *Proc. 7th Int. Workshop Cooperat. Inf. Agents (CIA)*, Helsinki, Finland, Aug. 2003, pp. 238–249.

[17] A. Ghosh, M. Mahdian, D. M. Reeves, D. M. Pennock, and R. Fugger, "Mechanism design on trust networks," in *Proc. 3rd Int. Workshop Internet Netw. Econ. (WINE)*, San Diego, CA, USA, Dec. 2007, pp. 257–268.

[18] W. Yuan, D. Guan, Y.-K. Lee, and S. Lee, "The small-world trust network," *Appl. Intell.*, vol. 35, no. 3, pp. 399–410, Dec. 2011.

[19] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic Web," *Web Semantics, Sci., Services Agents World Wide Web*, vol. 5, no. 2, pp. 58–71, Jan. 2007.

[20] J. Kohl and C. Neuman, "The kerberos network authentication service (v5)," Netw. Working Group, Digit. Equipment Corporation, MA, USA, Tech. Rep., 1993.

[21] L. Kagal, T. Finin, and A. Joshi, "A policy based approach to security for the semantic Web," in *Proc. 2nd Int. Conf. Semantic Web (ISWC)*, Sanibel Island, FL, USA, Oct. 2003, pp. 402–418.

[22] M. Carbone, M. Nielsen, and V. Sassone, "A formal model for trust in

dynamic networks," in *Proc. 1st Int. Conf. Softw. Eng. Formal Methods (SEFM)*. Brisbane, Australia, Sep. 2003, pp. 54–63.
[23] K. J. Stewart, "Transference as a means of building trust in world wide Web sites," in *Proc. 20th Int. Conf. Inf. Syst. (ICIS)*, Charlotte, NC, USA, Dec. 1999, pp. 459–464.
[24] K. J. Stewart and Y. Zhang, "Effects of hypertext links on trust transfer," in *Proc. 5th Int. Conf. Electron. Commerce (ICEC)*, Pittsburgh, PA, USA, Sep./Oct. 2003, pp. 235–239.
[25] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins, "Propagation of trust and distrust," in *Proc. 13th Int. Conf. World Wide Web (WWW)*, New York, NY, USA, May 2004, pp. 403–412
[26] V. Buskens, "The social structure of trust," *Social Netw.*, vol. 20, no. 3, pp. 265–289, Jul. 1998.
[27] R. Ashri, S. D. Ramchurn, J. Sabater, M. Luck, and N. R. Jennings, "Trust evaluation through relationship analysis," in *Proc. 4th Int. Conf. Auto. Agents Multiagent Syst. (AAMAS)*, Utrecht, The Netherlands, Jul. 2005, pp. 1005–1011.
[28] C. Bizer and R. Oldakowski, "Using context-and content-based trust policies on the semantic Web," in *Proc. 13th Int. Conf. World Wide Web-Alternate Track Papers Posters (WWW)*, New York, NY, USA, May 2004, pp. 228–229
[29] K. O'Hara, H. Alani, Y. Kalfoglou, and N. Shadbolt, "Trust strategies for the semantic Web," in *Proc. 3rd Int. Workshop Trust, Secur., Reputation Semantic Web (ISWC)*, Hiroshima, Japan, Nov. 2004, pp. 42–51.
[30] O.-J. Lee, M.-S. Hong, J. J. Jung, J. Shin, and P. Kim, "Adaptive collaborative filtering based on scalable clustering for big recommender systems," *Acta Polytech. Hungarica*, vol. 13, no. 2, pp. 179–194, 2016.
[31] O.-J. Lee, J. J. Jung, and Y. Eunsoon, "Predictive clustering for performance stability in collaborative filtering techniques," in *Proc. 2nd IEEE Int. Conf. Cybern. (CYBCONF)*, Gdynia, Poland, Jun. 2015, pp. 48–55.
[32] J. E. Jung, O.-J. Lee, E.-S. You, and M.-H. Nam, "A computational model of transmedia ecosystem for story-based contents," *Multimedia Tools Appl.*, To appear, doi: 10.1007/s11042-016-3626-5
[33] R. Levien, "Attack-Resistant Trust Metrics," in *Computing With Social Trust* (HumanŰComputer Interaction Series). London, U.K.: Springer, 2009, pp. 121–132.
[34] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic Web," in *Proc. 2nd Int. Conf. Semantic Web (ISWC)*, Sanibel Island, FL, USA, Oct. 2003, pp. 351–368.
[35] J. Golbeck, "Generating predictive movie recommendations from trust in social networks," in *Proc. 4th Int. Conf. Trust Manage. (iTrust)*, Pisa, Italy, May 2006, pp. 93–104.
[36] J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," *ACM Comput. Surv.*, vol. 46, no. 4, p. 44, 2014.
[37] I. Žliobaitė. (Oct. 2010). "Learning under concept drift: An overview." [Online]. Available: https://arxiv.org/abs/1010.4784
[38] J. E. Jung, M. Hong, and H. L. Nguyen, "Serendipity-based storification: From lifelogging to storytelling," *Multimedia Tools Appl.*, To appear, doi: 10.1007/s11042-016-3682-x
[39] T. T. Nguyen, H. L. Nguyen, D. Hwang, and J. J. Jung, "PageRank-based approach on ranking social events: A case study with Flickr," in *Proc. 2nd Nat. Found. Sci. Technol. Devel. Conf. Inf. Comput. Sci. (NICS)*, Ho Chi Minh, Vietnam, Sep. 2015, pp. 147–152.
[40] O.-J. Lee and J. E. Jung, "Sequence clustering-based automated rule generation for adaptive complex event processing," *Future Gener. Comput. Syst.*, vol. 66, pp. 100–109, Jan. 2017.
[41] N. H. Long and J. J. Jung, "Privacy-aware framework for matching online social identities in multiple social networking services," *Cybern. Syst.*, vol. 46, nos. 1–2, pp. 69–83, 2015.

HOANG LONG NGUYEN received the B.S. degree with the Department of Computer Engineering, Ho Chi Minh City University of Technology, Vietnam, in 2013, and the M.S. degree with the Department of Computer Engineering, Yeungnam University, South Korea, in 2016. He is currently pursuing the Ph.D. degree with Chung-Ang University, South Korea. His research topics include knowledge engineering on social networks by using machine learning, semantic Web mining, and ambient intelligence.

O-JOUN LEE received the B.Eng. degree in software science from Dankook University in 2015. He is currently pursuing the combined M.S. and Ph.D. degrees with the School of Computer Engineering, Chung-Ang University, South Korea. His research topics are recommendation system on digital content by using sequential pattern mining, incremental clustering, and social network analysis.

JAI E. JUNG received the B.Eng. degree in computer science and mechanical engineering, and the M.S. and Ph.D. degrees in computer and information engineering from Inha University in 1999, 2002, and 2005, respectively. He was a Post-Doctoral Researcher with INRIA Rhone-Alpes, France, in 2006, and a Visiting Scientist with the Fraunhofer Institute, Berlin, Germany, in 2004. He has been an Assistant Professor with Yeungnam University, South Korea, since 2007. He has been an Associate Professor with Chung-Ang University, South Korea, since 2014. He has been involved in intelligent schemes to understand various social dynamics in large scale social media (e.g., Twitter and Flickr). His research topics are knowledge engineering on social networks by using many types of AI methodologies, such as data mining, machine learning, and logical reasoning.

JAEHWA PARK received the B.S. and M.S. degrees in electronic engineering from Hanyang University, Seoul, South Korea, in 1989 and 1991, respectively, and the Ph.D. degree in electrical engineering from The State University of New York at Buffalo in 2000. He was a Research Staff with the Center for Document Analysis and Recognition, Buffalo, NY, and the Lexicus Division of Motorola Inc., Palo Alto, CA, USA. He is currently a Professor with the Department of Computer Science and Engineering, Chung-Ang University, Seoul. His research interests include cognitive pattern recognition and autonomous machine learning.

TAI-WON UM received the Ph.D. degree from the Korea Advanced Institute of Science and Technology, South Korea. He is currently a Senior Researcher with the Electronics and Telecommunications Research Institute, South Korea. His research interests include trusted information infrastructure, Internet of Things, and smart media platforms and services.

HYUN-WOO LEE received the M.S. and Ph.D. degrees from Korea Aerospace University in 1995 and 2005, respectively. He is currently an Assistant Vice President of the Media Research Division, Electronics and Telecommunications Research Institute. His main research interests include smart media, tera-media, and open screen service platforms. His current research interests also include trusted information infrastructure for realizing trustworthy IoT eco-system.