electronics

MDPI

Article

A Trustworthy SIoT Aware Mechanism as an Enabler for Citizen Services in Smart Cities

Ateeq Ur Rehman [1], Rizwan Ali Naqvi [2], Abdul Rehman [3], Anand Paul [3,*], Muhammad Tariq Sadiq [4] and Dildar Hussain [5,*]

1 College of Internet of Things Engineering, Hohai University, Changzhou 213022, China; ateqrehman@gmail.com
2 Department of Unmanned Vehicle Engineering, Sejong University, 209, Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea; rizwanali@sejong.ac.kr
3 Department of Computer Science and Engineering, Kyungpook National University, Daegu 41566, Korea; a.rehman.iiui@gmail.com
4 School of Automation, Northwestern Polytechnical University, 127 West Youyi Road, Xian 710072, China; tariq.sadiq@mail.nwpu.edu.cn
5 School of Computational Sciences, Korea Institute for Advanced Study (KIAS), 85 Hoegiro Dongdaemun-gu, Seoul 02455, Korea
* Correspondence: paul.editor@gmail.com (A.P.); hussain@kias.re.kr (D.H.)

Received: 22 April 2020; Accepted: 29 May 2020; Published: 1 June 2020

Abstract: In the recent era, new information technologies have a significant impact on social networks. Initial integration of information and communication technologies (ICT) into city operations has promoted information city, ease of communication and principles of smart communities. Subsequently, the idea of the Internet of Things (IoT) with the specific focus of social IoT (SIoT) has contributed towards the smart cities (SC), which support the city operations with minimal human interaction. The user-generated data obtained by SIoT can be exploited to produce new useful information for creating citizen-centered smart services for SC. The aim of this research is twofold. Firstly, we used the concept of local and global trust to provide new services in SC based on popular online social networks (OSN) data used by the citizens. Secondly, the sustainability of the three different OSN is assessed. This paper investigates the social network domain with regard to the SC. Although in SC, OSN are increasing day by day, there is still an unresolved issue of trust among their users and also OSN are not much sustainable. In this research, we are analyzing the sustainability of different OSN for the SC. We employ datasets of three different social networks for our analyses. A local trust model is used to identify the central user within the local cluster while the global trust-based framework is used to identify the opinion leaders. Our analysis based on the datasets of Facebook, Twitter, and Slashdot unveil that filtration of these central-local users and opinion leaders result in the dispersion and significant reduction in a network. A novel model is being developed that outlines the relationship between local and global trust for the protection of OSN users in SC. Furthermore, the proposed mechanism uses the data posted by citizens on OSN to propose new services by mitigating the effect of untrusted users.

Keywords: social internet of things; global trust; local trust; opinion leader; communication in smart cities

1. Introduction

The Internet of things (IoT) is a technology that assimilates a vast amount of ubiquitous and heterogeneous objects which generate information about the physical world continuously. Such objects tend to communicate and provide several services previously inconceivable. These objects are also

known as smart objects [1], as they provide information about the real-world with minimum human intervention. These smart objects may include an actuator, a smartphone, a sensor, a general computer, etc. The information from smart objects is accessible via standard web browsers and many other platforms that offer application programming interfaces (APIs) to retrieve data from sensors and actuators. One real application of IoT-enabled scenarios is the smart city (SC).

Nowadays, there has been a lot of research activities that investigate the possibilities of incorporating social networking concepts into IoT solutions. The resulting model is termed as the social internet of things (SIoT) [1]. IoT enabled applications have a huge impact on the environment and on the way humans interact with their surroundings, thus security is the crucial point. In SC, the objects interact with both humans and smart devices in multiple fashions. Considering this, it is a rational decision to connect smart city objects with online social networks (OSN), although this integration results in multiple security issues. OSN are the platform where both devices and humans can exchange information, being an information source, and sink for the SC objects. SC objects must provide information to both users and devices rendering integration with the social networks being a logical move.

Recently, the use of OSN has increased dramatically and is a ubiquitous part of the modern era. Initially, these platforms used to establish communication links between individuals or small groups. Recently, however, these platforms not only provide its users the possibility to express themselves and remain in touch with friends, but have also been updated with the latest trends, business strategies, and also the latest news around the globe. Among the various OSN, Facebook has drawn much attention. A study from America revealed that in May of 2011, internet users from America spent around 53,500 million minutes on Facebook [2]. In addition, by March of 2018, Facebook had around 2.2 billion monthly active users [3]. In total, Facebook users have more than 150 billion friend connections and on average upload more than 350 million Facebook photos each day [4].

Slashdot is a prominent technology-oriented news-sharing website launched in 1997 that regularly publishes short news posts and allows its users to comment on them. In Slashdot, every comment can be rated between the scale of −1 to +5 based upon the community's feedback [5]. Slashdot not only shows the score of each post but also helps users to order or select the messages available depending on the score [6].

Twitter is also a very famous social networking platform with more than 300 million active users in a month and around 500 million tweets are posted on a daily basis [7]. Among Twitter users, 40% are technical users [8]. The most popular active users are political leaders, scientists, and celebrities who use Twitter to share their opinion and achievements [9]. Twitter users can post short messages which are called tweets and can follow other Twitter users. In addition, users can mention, reply, and retweet. Among these, a retweet is a very interesting activity as user shares and acknowledges the contents posted by other users. During the retweet, the originality of the tweet and its original user's identity remains unchanged and the users agree with the content of the original tweeter. The user within the social networks built the social capital by engaging with others, e.g., by getting friend with someone, commenting on the posts of others, commenting on the comments, etc. The social capital is aimed at creating an interaction climate within the users of the social network.

OSN are coming up with a promising paradigm to influence users. However, the increase in access to these OSN have put both users and their devices at risk of privacy. Some of the malicious actions may include fake profiles (Socialbots) in the OSN [2,4], de-anonymization attacks [4], identity clone attacks [4], information leakage [4], Socware [4], cyberbullying [4], cross-site scripting (XSS) [4], social phishing [10], spams in the tagging system [11], etc. Keeping the constraint of privacy, there is a need for trust communities so that the users can communicate without any risk of fraud and being hacked. It is worth studying how to give a user an accurate trust assessment on others before he/she interacts with them.

A trust model for OSN in [12,13] and the SocialTrust framework has been proposed in [14,15]. A social trust-based knowledge-sharing willingness modeling is undergone in [16]. According to the

authors in [3], over the past decade, even the largest OSN have sometimes collapsed. The collapse of an OSN iWiW (Hungarian popular online social media platform accounted for almost 30% of the nation's population) is being investigated in [3] by successfully modeling diffusion and churn on the network.

OSN are very useful resource for getting information about the city. Public administrators and policymakers are using the OSN data to know the people's opinions about the city. This data is like an ornament for local government officials and can be used in city planning and development [17]. Moreover, the data used by an individual as well as by the community can be used to propose new services for the SC.

The work in this research is mainly focused on looking at how a social network is formed and what network structures are likely to emerge as many OSN are not successful because of the limited number of users and minimum interactions among these users. This work investigates a new trust model for OSN. This trust model considers the interaction relations and trust value for everyone in OSN. The framework of trusted communities is formed by considering the factors of local and global trust. The factor of trust is used to mitigate the mixing of fake data by untrusted third parties. The publically available datasets of Facebook, Twitter, and Slashdot are used to study the structure and sustainability of the OSN.

The organization of the paper is as follows. Section 2 reviews the literature. Details about the proposed trust models are presented in Section 3. Section 4 describes the social network datasets adopted in this paper. A brief discussion part along with results are included in Section 5. Finally, Section 6 concludes the paper.

2. Background and Related Work

The text in this section briefly explains the current state of the art knowledge on Social IoT, OSN, the factor of trust in OSN, the role of trust in SC, and the deployment of OSN in informational urbanism.

2.1. The Concept of Social IoT

The IoT integrates the huge number of homogeneous and heterogeneous objects. Social IoT can be described in terms of IoT [1]. Social IoT is the integration of social networking with IoT objects. In SIoT, objects become socially connected and smart to have many common benefits [18]. These objects interact with other objects based on their owners or manufacturers [18]. Further, these objects have the potential to advertise their existence in the network that subsequently contributes to provide several services. These objects are versatile and thus can conveniently move in the network. Therefore, we infer that billions of objects in IoT can discover and spread out the information and services in a trustworthy manner.

The concept of convergence of IoT and social networks is getting momentum day by day because of its potential that SIoT would carry various implications soon when the world will be highly congested with numerous smart objects. The SIoT mimics human behavior in making interaction, network navigability, and in seeking the required services [1].

2.2. Analysis of Online Social Networks

Around the end of the 20th century, the revolution of the internet impacted considerably in almost every domain of people's life. Easy access to internet facilities had a huge influence on the growth of social networks [8]. According to the statistics report produced in January 2020, the number of active users of famous social networks are shown in Figure 1. Among all social networks, Facebook is the most popular with 2449 billion active users. Twitter is ranked in the thirteenth position with 340 million active users. The statistics shown in Figure 1 are of vital significance as these demonstrate how drastically, the social media and its users are increasing day by day. Social media and its implementation have revolutionized the internet and shifted the mode of communication by enabling dynamic connections between individuals and organizations. Astonishingly, only Facebook messenger and WhatsApp handle around 60 billion messages every day [19]. OSN provide services to meet a broad range of

social and commercial needs such as publishing, networking, collaborating, discussing, messaging, and sharing, etc., as shown in Figure 2. Facebook, Twitter, and Google are in the center of the figure to show that all of the online services grow around them [20].

Social networks are of major importance for an individual when they serve his/her purpose. The author in [21] has done a study on membership size, communication activity, and sustainability of the online social structures. In addition, social networks can be sustainable on a long term basis by providing positive benefits (e.g., friendship, knowledge sharing, encouraging discussion, quick access of latest information, social and emotional support, and supporting teamwork such as political campaigns, etc.) to its users.

2.3. The Concept of Trust in Online Social Networks

Trust is an important topic for online activities since it relates to knowledge of decision-making and social interaction. The authors in [22] used the fuzzy-based model to compute reputation and trust. Homophily is exploited in [23] to built hTrust framework for trust prediction. Local trust is used by [24] to form social structures in the virtual communities. A novel framework LOCABAL has been proposed in [25] considering both local and global social relations by deploying matrix factorization.

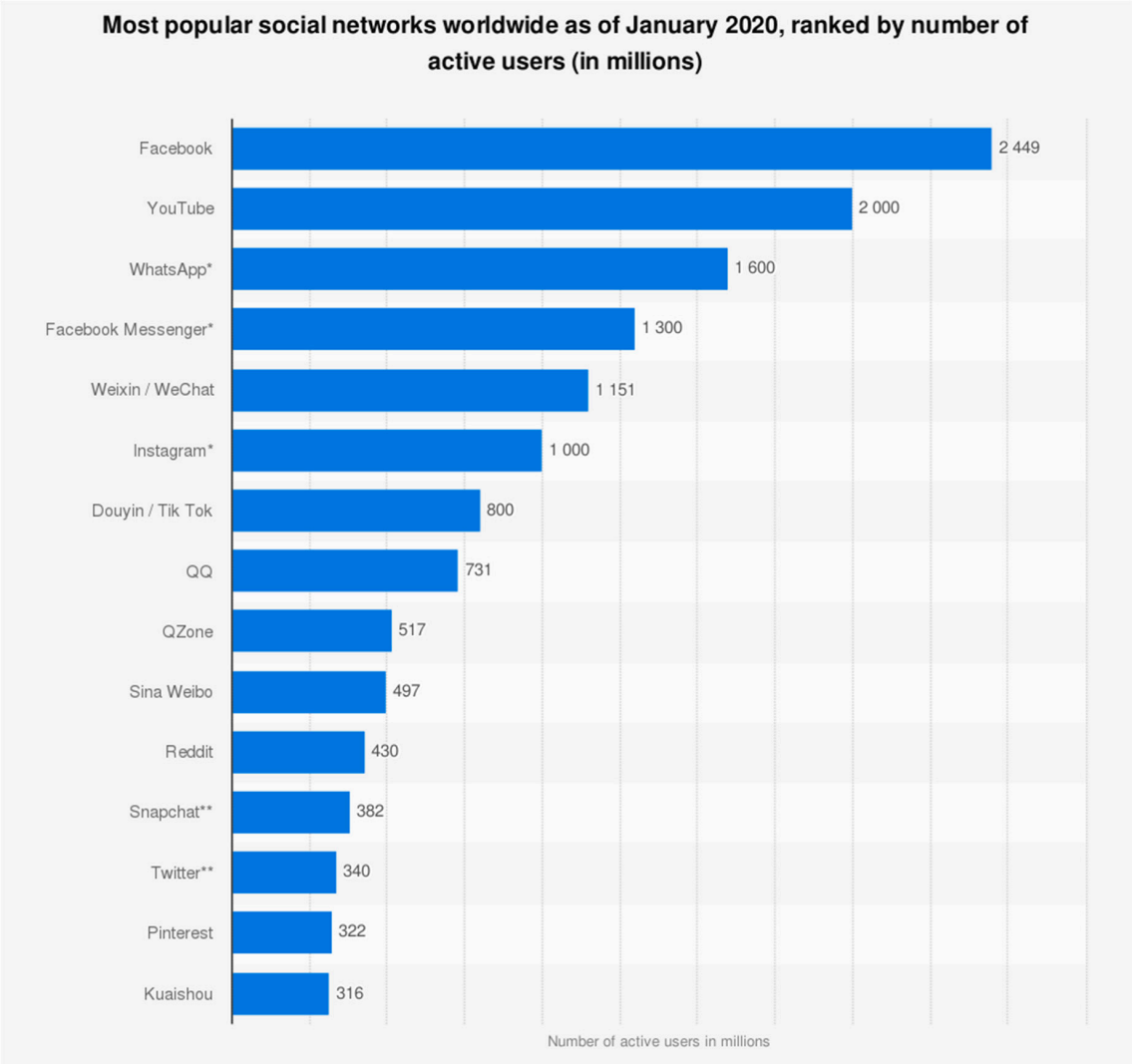

Figure 1. The number of active users of social network sites (January 2020) [26].

Figure 2. Social media landscape [20].

Trust metrics measure the quantitative estimate of how much trust an agent 'a' can give to its peer 'b', taking into consideration the trust ratings on the network from other users. These metrics will always work purposefully, not give excessive trust to individuals or agents whose trustworthiness is uncertain. Basically, trust metrics may be subdivided into ones with global, and others with local scope. Global trust metrics consider all peers and the trust links connecting them. Global trust ranks are assigned to a user based upon the information of the complete trust graph. On the other hand, trust metrics with local scope consider personal bias. Furthermore, the authors in [27] claimed that only local trust metrics are 'true' trust metrics as the global trust metrics consider the overall reputation despite personalized trust.

The plethora of trust metrics can be classified as shown in Figure 3. The trust propagation can be in a centralized or distributed manner. For centralized networks, the counts of positive/negative feedback on the posts, community of interest (CoI), and friend requests are some of the criteria that can be used to evaluate the global trust of an individual. For decentralized networks, for example, shalshsot.org which allows everyone to create content and there is a lack of central quality control, evaluation of contents becomes a challenge [28].

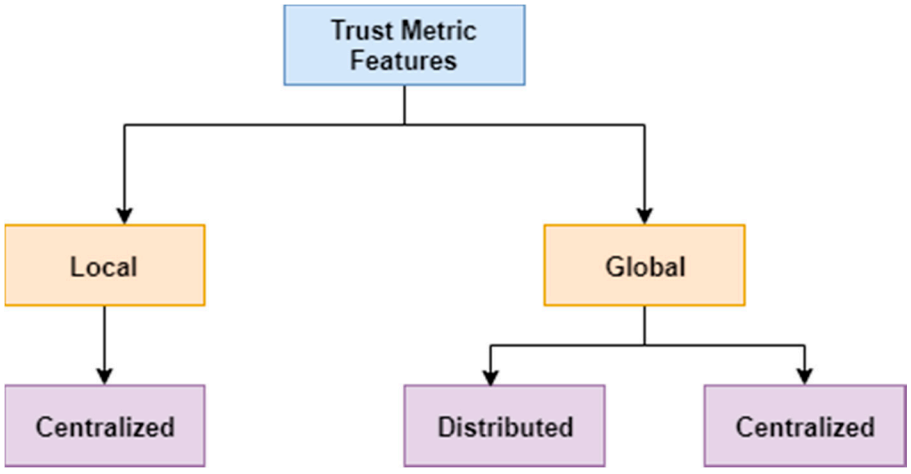

Figure 3. Classification of trust metric.

In directed networks, a user can connect without the assent of the second user, for example, Twitter. Whereas, in undirected networks such as Facebook, the willingness of the second user is essential for friendship approval. In undirected systems, edges are mutual, consequently, assent is required from both endpoints. Therefore, undirected models are appropriate for some types of monetary and social connections. For directed networks, a vertex can connect straightforwardly to another without prior permission. Consequently, directed models are progressively appropriate for catching communications that are latent one way [29]. In our research, we have used both direct and indirect networks.

2.4. The Role of Trust in Smart Cities

The metropolitan world is becoming ever more connected and dynamic. We would be overwhelmed in the coming decades by trillions of IoT sensors, computers, and machines. Cities and metropolitan regions benefiting from the IoT are widely recognized as SC. Based on the increase in IoT adoption worldwide, potential city situational awareness and management strategies would depend in part on SC technologies. Actually, the objects in IoT belong to humans in the network, which is the concept of the SIoT [1,30]. SIoT is, therefore, known as social networks through which any device, according to its users, is able to create social ties with others. SC being equipped with billions of IoT devices and their social ties have serious concerns of security, trust, and privacy. In SC, we will be more reliant on IoT devices to make our own decisions.

When devices use data from other devices in the network to make decisions, they need to learn how to trust that data as well as the devices/objects they are interacting with. Trust is the belief that a device or system has the ability to function accurately, safely, and efficiently within a defined context [31]. Therefore, the participating IoT devices in the smart city must adopt the trust management mechanism to guarantee the quality of the assistance behavior of intelligent devices and enhance the satisfaction of the users. The lack of trust may influence the adoption of sharing data in SC. The objective of this work is to provide a trustworthy mechanism for the citizen of SC that enables the induction of new services by mitigating the risk of fraud.

2.5. The Exploitation of Online Social Networks in Informational Urbanism

The world is continuing to urbanize and sixty percent of the world's population is expected to be urban by 2030 [32]. In the area of informational urbanism, public authorities are very keen on gaining the views of people about the city. In this way, it becomes easier for people to participate in public decision-making processes by posting their opinions on OSN [33].

Big data analytics (BDA) have posed emerging challenges in the area of social network analysis (SNA), especially how the OSN data can be interpreted and used to obtain useful information regarding people and city operations. BDA helps policymakers in making prediction models, uncover behavior trends and analyze citizen satisfaction as well as accelerate the urban sustainability research, planning, and development [34]. In this perspective, OSN and SC are of keen interest to both the policymakers and citizens. OSN contribute to the SC administration as these platforms collect the data of citizens for officials. In addition, SC serve an important opportunity for technology firms like Uber, Didi, and Airbnb, etc. which are rapidly involved in city management [35].

Twitter is one of the most widely used platforms nowadays. Authors in [36] collected 15,000 tweets by exploiting natural language processing (NLP) while considering the main areas of knowledge of topics where the concept of sustainability was used. Furthermore, they mapped the social network of users who created or disseminated content regarding 'sustainability' on Twitter during the observation period. The collected tweets were used to analyze the sentiments of the participants regarding the concept of sustainability. Further, Twitter is used in [37] to examine the factors affecting the outdoor activities of humans in cities such as climate updates and traffic congestion.

3. Materials and Methods

3.1. Trust Model for Social Network

The concept of trust is not new as many researchers have worked on trust in different fields including computer science [38], economics [39], sociology [40], psychology [41]. Trust can be described as a trustee's belief that the trustee will deliver or achieve a trust goal as the intention of the trustee denoted by T_{ij} generally represented as a function:

$$T_{ij} = f\left(t_{ij}, t_{ji}, r_{ij}^{k}, g_j, l_i\right) \tag{1}$$

where t_{ij} and t_{ji} represent the trust between two actors (trustor and trustee), r_{ij}^{k} are the recommendations of ith actor to jth actor about trust to kth actor, g_j is the reputation or global trust of jth actor and l_i is the nature of the trust of ith actor. T_{ij} is made up of two components:

$$T_{ij} = t_{ij} + \Delta t_{ij} \tag{2}$$

where Δt_{ij} changes in the previous value of trust and is represented by:

$$\Delta T_{ij} = \sqrt{t_{ij} t_{ji}} r_i^j w_r g_j w_g l_i w_l \tag{3}$$

Thus, t_{ij} is the previous value of trust of ith actor in the jth, and t_{ji} is the previous value of trust of jth actor on ith one. r_i^j are the average recommendations about jth to ith actor given by

$$r_i^j = \frac{\sum_1^n t_{ik} t_{kj}}{n} \tag{4}$$

g_j represents the global trust or reputation of the jth actor as given by

$$g_j = \frac{\sum_1^m r_j}{m} \tag{5}$$

where r_j represents the rating values given by the m users.

The effect of local trust, global trust, and recommendation values are decided by the respective weight coefficients w_l, w_g, and w_r ranging in the interval [0, 1]. Re-arranging Equations (2), we have:

$$T_{ij} = t_{ij} + \sqrt{t_{ij} t_{ji}} \left(\frac{\sum_1^n t_{ik} t_{kj}}{n} \right) w_r \left(\frac{\sum_1^m r_j}{m} \right) w_g l_i w_l \tag{6}$$

3.2. Local Trust

Local trust means that, if node A trusts node B, it does not change its opinion considering the fact that node C does not trust node B [42]. For example, if two users are talking in the context of restaurant selection to find quality food, users A and B may have a similar opinion built upon trust among them but a third user may have different opinion contradicting with one or both users. However, all three nodes may agree on the selection of a cinema to watch a movie. The author in [43] proposed an algorithm to infer a similar sort of trust in social networks. Therefore, while building trustworthy communities, it is very important to consider that in which context the users were deciding about. The trust can be positive or negative, mathematical modeling of local trust is given in the following equations:

$$\left| LT_{ij}^{x+} \right| = \sum_{n=1}^{|N|} +1 \tag{7}$$

$$\left|LT_{ij}^{x-}\right| = \sum_{n=1}^{|N|} -1 \tag{8}$$

$$LocalTrust\left(f_i^x\right) = \frac{\sum_{j=1}^{|N|-1} \frac{\left|LT_{ij}^{x+}\right|}{\left|LT_{ij}^{x+}\right|+\left|LT_{ij}^{x-}\right|}}{|N|-1} \tag{9}$$

$$LocalTrust\ (f_i) = \frac{\sum_{x=1}^{|X|} LocalTrust\left(f_i^x\right)}{|X|} \tag{10}$$

3.3. Global Trust

Global trust is also known as reputation [44]. Every node/member has its trust value in a network and it is in the knowledge of every other node within the local network. The reputation of a node relates to the node's trustworthiness from the viewpoint of other nodes of the network.

Mathematical modeling of global trust is given in Equations (11)–(14). Suppose that F is the set representing the users within the network and $\left|GT_{ij}^{x+}\right|$ denotes the positive interactions that a user $f_i \in F$ has with the user $f_j \in F$ considering in the context of global trust.

$$\left|GT_{ij}^{x+}\right| = \sum_{n=1}^{|N|} +1 \tag{11}$$

$$\left|GT_{ij}^{x-}\right| = \sum_{n=1}^{|N|} -1 \tag{12}$$

where $|N|$ represents the total number of activities.

The global trust for an individual $f_i \in F$ is then given by:

$$GlobalTrust\left(f_i^x\right) = \frac{\sum_{j=}^{|M|-1} \frac{\left|GT_{ij}^{x+}\right|}{\left|GT_{ij}^{x+}\right|+\left|GT_{ij}^{x-}\right|}}{|M|-1} \tag{13}$$

$$GlobalTrust\ (f_i) = \frac{\sum_{x=1}^{|X|} GlobalTrust\left(f_i^x\right)}{|X|} \tag{14}$$

The trust of an individual f_i in the community is then represented by:

$$Overalltrust(f_i) = a.globaltrsut(f_i) + \beta.localtrsut(f_i) \tag{15}$$

where a and β are the weighting parameters in $[0, 1]$ and $\beta = 1 - \alpha$.

3.4. Proposed Trust Based Model for Smart Cities

In this advanced and ICT-equipped era, several standardization bodies including ITU, ISO, etc. and researchers are assessing the performance of SC from various perspectives. ITU SC Focus Group has presented three performance measures for the sustainable SC which are (i) equity and social cohesion (ii) quality of life (iii) physical infrastructure, which are being accessed by the respective indexes [45]. Due to the broad scope of SC' aspects, the vast volume of urban data is needed to recognize the local needs and to build, manage and operate the smart services [46].

Data generated by the use of OSN is turned into useful information for SC which in effect contributes to the creation of new services to enhance life quality and, ultimately, the advancement of smart living as demonstrated in Figure 4. Besides, mistrust and malicious activities towards OSN discourage social interaction and result in the entry of fake data, which in effect influence social

engagement and diminishes the performance of corresponding new services. In addition, local trust at an individual level can affect the global trust in SC and vice-versa as depicted in Figure 4. Moreover, the level of local awareness, their action, and perception towards data provisioning determines that in SC it impacts cyber protection positively or negatively.

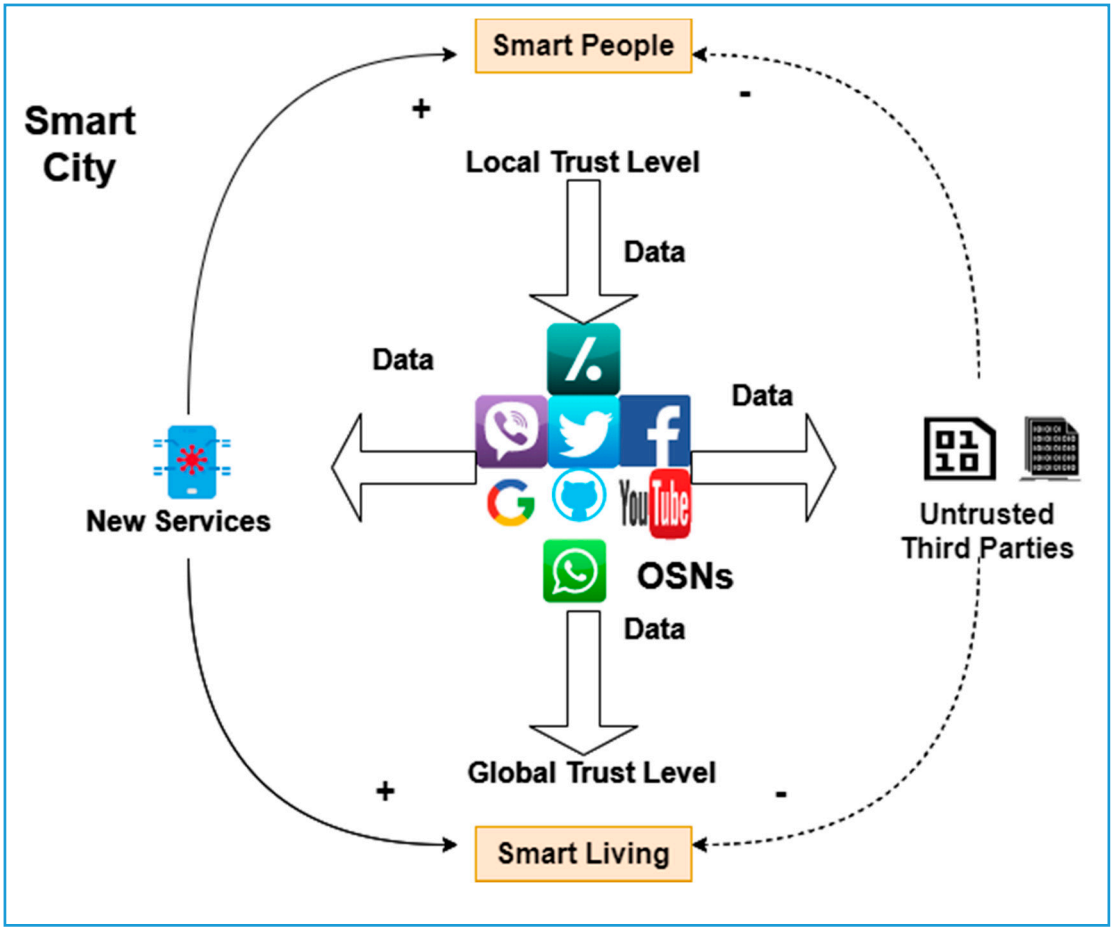

Figure 4. Local Versus global trust-based mechanism in smart cities.

3.5. Local and Global Trusted Users

In Figure 5, two users A and B have a cluster of users surrounding them. The local central users A and B in each cluster are more trusted users as compared to the other users within the network ($\alpha = 0$) because all users trust these central users. For the local central user, the direct interaction (trust relationship) between the local central user and other common users of the cluster is compulsory. This interaction helps the local central user to avoid the trust-related attacks. These attacks may include self-promoting attacks, bad-mouthing attacks, ballot stuffing attacks, discriminatory attacks, etc., details of the trust-related attacks is given in [44]. A local trusted user has a high value of trust among all the users of the cluster.

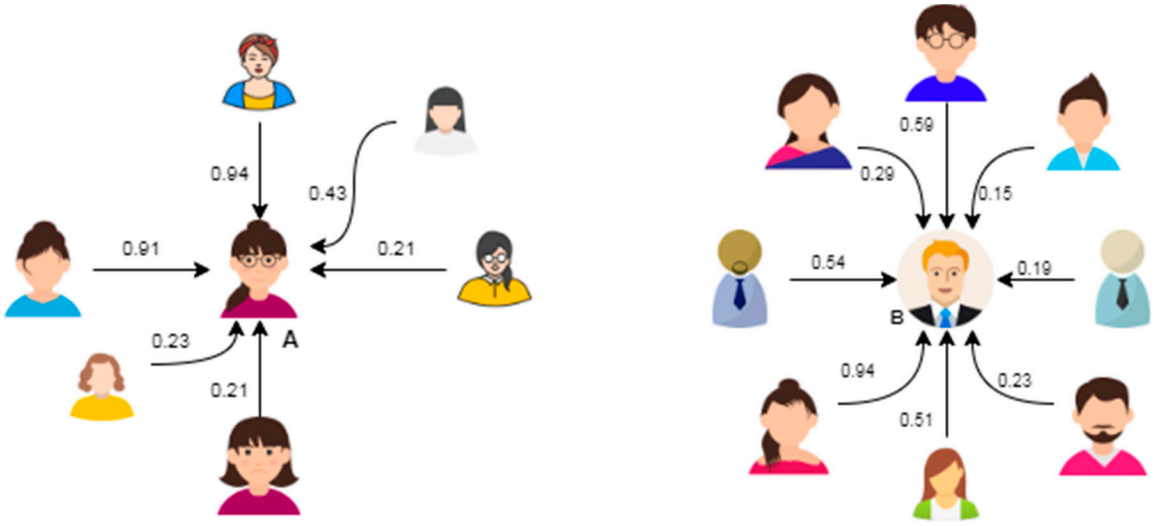

Figure 5. An illustration of a trust network for the local central users.

As there are many clusters even within a small social network and if a user in a local cluster does not have any information about the trust value of a user residing in some other cluster. It is convenient for us to follow the suggestion from the one with a good reputation. The global trusted user as introduced in Figure 6 will share the trust value of the users among each other as the global trusted user who is an opinion leader has the information of all users through the local trusted users. A global trusted user is trustworthy for giving the details of other user's trust values and opinions about specific contexts or events. According to the proposed model ($\alpha = 1$), which means that an overall global trusted user has a high value of trust but high followers. For a global trusted user, prevailing the trust with each individual user of the local cluster is not required and only the central-local users are enough to create the strong relation of trust among a global user and other users of the cluster.

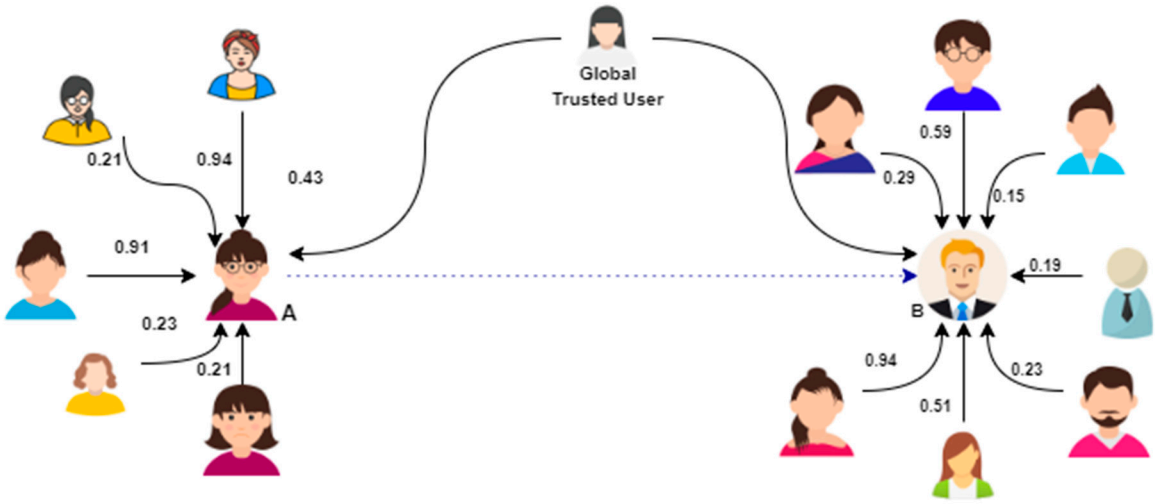

Figure 6. An illustration of a trust network for the global central user.

4. Dataset Description

Three datasets are used in order to study the pattern of social networks. The datasets are described below and profiles of used datasets are given in Table 1.

Table 1. Summary of statistics of the datasets utilized in experiments.

Dataset	Nodes	Edges	Directed	Modularity	Average Degree	Average Path Length	Average Clustering Coefficient	Network Diameter
Slashdot	82,168	948,464	yes	0.327	11.543	11.281	0.511	13
Twitter	465,107	834,797	yes	0.643	1.795	6.919	0.01	19
Facebook	4039	88,234	No	0.834	21.846	3.693	0.617	8

4.1. Slashdot

For the evaluation of our proposed research problem, the dataset of a social networking website named Slashdot [47] is used. It is a news-sharing website founded in 1997. It contains content submitted by users and reviewed by editors. In 2002, the Zoo feature was added on the website, which is used to tag users as friends or foes. The network contains 82,168 nodes and 948,464 edges/links among the friends or foes. In addition, Slashdot is on the few social networking websites which allow users to negatively rate other users as opposed to most other social networks.

4.2. Twitter

A directed Twitter network containing information about who follows whom is used in our experimentation. The dataset contains 465,107 nodes, 834,797 edges, 25,378,846 tweets and was originally collected by the [48].

4.3. Facebook

This dataset contains information of 10 ego-networks, 193 circles and 4039 users [49]. The data has been anonymized.

The statistics provided in Table 1 are illustrated as follows:

- Edges: A graph consists of nodes and edges. An edge connects two nodes or connects a node to itself.
- Directed vs. Undirected Graphs: A graph composed of directed edges is the directed graph while the undirected graph is composed of undirected edges.
- Modularity: The set of nodes that interact with each other more frequently than expected by random chance. The modularity values for the Slashdot, Twitter, and Facebook networks are 0.327, 0.643, and 0.834, respectively. The strength of information dissemination is high when the modularity value is high.
- Average Degree: Degree is the number of edges connected to a node. Average degree in this context implies that there are about 11.281 edges for one node in the Slashdot network, or more textually that implies that each person on Slashdot has about 11 friends or foes.
- Average Path Length: It is the average number of steps along the shortest paths for all possible pairs of nodes in the network.
- Clustering Coefficient: It is the ability of nodes in a graph to cluster together with neighbors. A high average cluster coefficient means a node's friends tend to know one another. The average clustering coefficient of the Facebook dataset is 0.617 which is high as compare to Slashdot and Twitter. This high value means that there is high clustering among the nodes. This, in turn, implies the high friendship relations among the high degree nodes.
- Network Diameter: A graph's diameter is the largest number of nodes which must be traversed in order to travel from one node to another when paths which backtrack.

5. Results and Discussion

In this work, we proposed our local and global trust-based models to identify the significance of local and global central users. To validate the proposed method, the experiments were performed by

using the publically available datasets of common social networks including Facebook, Twitter, and Slashdot. The datasets have been previously used by [47] to study the community structure for a large network, by [48] to discover the information diffusion in social media, by [50] by using small-world phenomena in SIoTs, and by [49] to discover the social circles in ego network. The core objective to use different datasets is to analyze the proposed model by using different settings. A brief description of the used datasets is summarized in Table 1.

Most trusted users who are identified on the basis of highest betweenness centrality (BC) values are termed as the opinion leaders [9,51]. The in-degree, out-degree, and betweenness centrality measures of top three users for each network are shown in Table 2. For the Facebook network, the ego network of depth one for the user ranked at position one with ID 107 has an in-degree centrality of 2, out-degree centrality value 1043, and betweenness centrality value of 3,916,560.1444. The ego-network for this user is demonstrated in Figure 7a. For the Twitter network, the user with ID 14654 is the identified opinion leader as shown in Figure 7b with the in-degree, out-degree, and betweenness centrality values of 47,499, and 47,435,239.071 respectively. Similarly, the user bearing the ID 2494 is the opinion leader for the Slashdot network as depicted in Figure 7c. This user has an in-degree value of 2553, an out-degree value of 2511, and betweenness centrality of 282,890,149.429. The nodes with ID 107, 14,654, and 2494 in the case of Facebook, Twitter, and Slashdot respectively have most control over the network as most of the information passes through these nodes. Figure 7 shows the ego-networks for these users which are highly ranked in all the networks. Definitely, multiple opinion leaders exist even within a single network.

Table 2. The betweenness-wise rank of central users found in each network.

Dataset	Node ID	In-Degree	Out-Degree	Betweenness	Rank
Facebook	107	2	1043	3,916,560.144	1
	1684	14	778	2,753,286.686	2
	1912	7	748	1,868,918.212	3
Slashdot	2494	2553	2511	282,890,149.429	1
	4805	2292	2248	267,207,834.401	2
	398	2355	2209	246,920,860.158	3
Twitter	14654	47	499	47,435,239.071	1
	8846	63	498	44,448,945.858	2
	7011	37	497	41,698,444.409	3

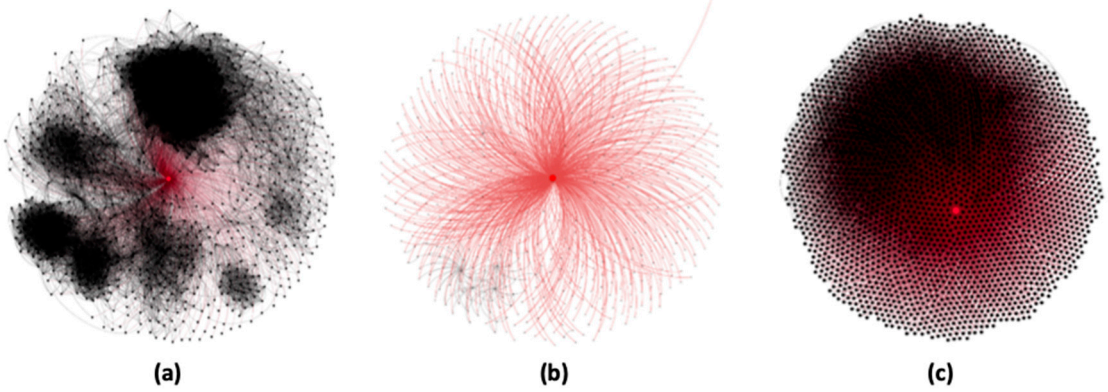

Figure 7. Ego network of degree one for the opinion leaders of (**a**) Facebook, (**b**) Twitter, and (**c**) Slashdot.

Datasets are visualized in Gephi [52,53], by deploying the Yifan Hu algorithm [54] on the Facebook dataset, MultiGravity FroceAtlas 2 algorithm [55] on the Twitter dataset and Yifan Hu Proportional algorithm on Slashdot dataset. The Yifan Hu Proportional algorithm has much resemblance to the Yifan Hu algorithm, the only difference is that it uses a proportional strategy for the placement of

nodes. Graph visualization of the whole network for Facebook, Twitter, and Slashdot social networks are shown in Figures 8a, 9a and 10a respectively.

Authors in [9,42,51,56] used the betweenness centrality as a measure to rank the users within the network and also to find the opinion leaders existing in the network based on the values of BC. In our work also, users are ranked in each network based on their BC values as shown in Table 2. Where BC demonstrates how often a node appears on the shortest paths between nodes in the network. From each network, the top three most trusted nodes have been selected based on the high BC values as demonstrated in Table 2. We are now removing these highly trusted users from the networks and looking at the effects of these removals on the overall network sustainability. After removing the local and global users (i.e., the opinion leaders) from the network structure, many users clustered with these highly trusted users disappear from the network.

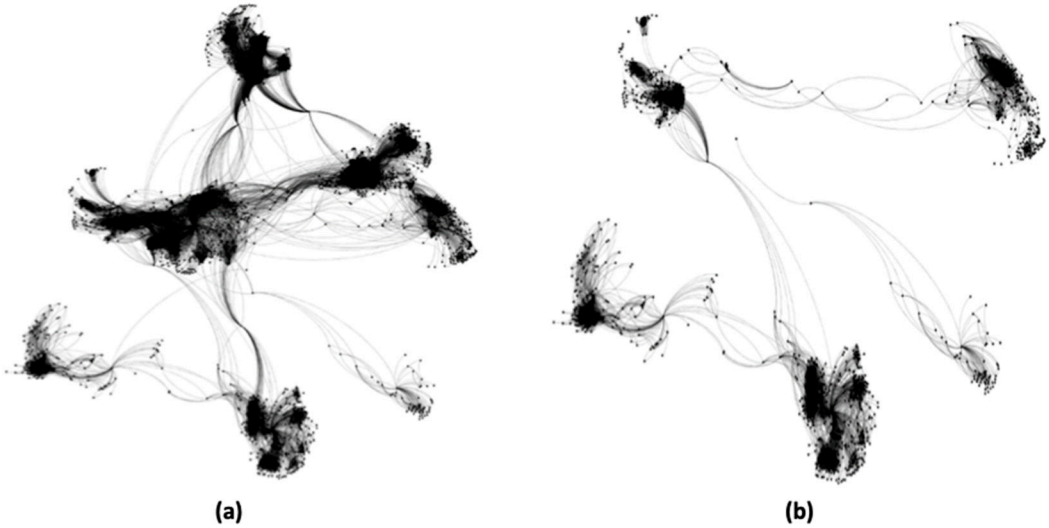

Figure 8. (**a**) Visualization of the full network of the Facebook dataset by deploying the Yifan Hu algorithm, and (**b**) filtered network (only 36.3% nodes and 15.04% edges are visible).

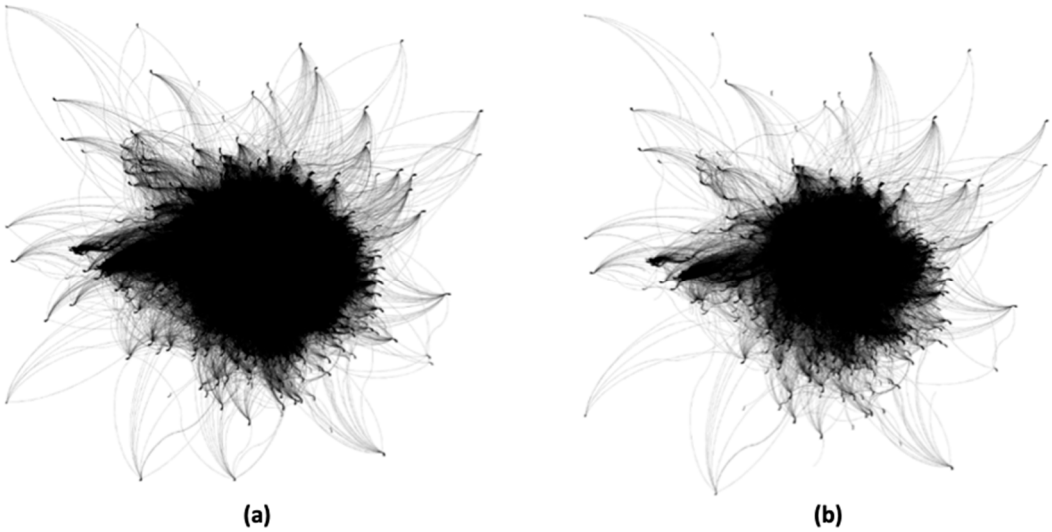

Figure 9. (**a**) Visualization of the full network Twitter by deploying the MultiGravity FroceAtlas 2 algorithm, and (**b**) filtered network (only 90.03% nodes and 25.25% edges are visible).

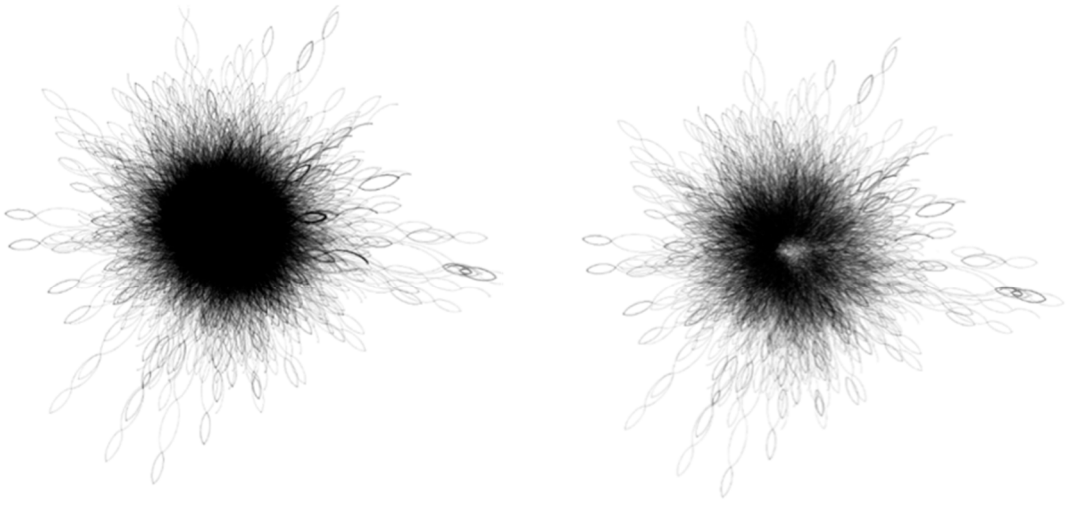

Figure 10. (**a**) Visualization of the full network of Slashdot by deploying the Yifan Hu Proportional algorithm, and (**b**) filtered network (only 43.32% nodes are visible).

The interconnection of a node with other nodes can be visualized by its ego-network as shown in Figure 7a–c. In order to evaluate our proposition, a filter was applied to all three datasets. Although, for all three networks, the applied filter composed of the intersection of three conditional parameters but the selection of opinion leaders and their corresponding ego-networks along with the depth vary for each OSN. For each condition, the NOT operator is the main filter and ego-network is the sub-filter under the NOT operator. For the Facebook network, the filter is composed of intersection of three conditional parameters which are (a) negation of ego-network of a node having ID 1912, (b) removal of ego-network of a node having ID 1684, and (c) excluding the ego-network of ID 107. The result of filtration is shown in Figure 8b in which only 36.3% nodes and 15.04% edges are remaining as compared to the original network.

The filter applied to the Twitter network is composed of the intersection of three conditions including (a) NOT operator applied on the ego-network with ID 14654, (b) NOT operator in combination with ego-network of ID 8846, and (c) deployment of NOT operator with the ego-network of node ID 7011. The result is shown in Figure 9b. In a similar way, the filtration is applied to the dataset of Sladhdot social media but on the ego-networks of the nodes with ID 2492, ID 398, and ID 4805 as demonstrated in Figure 10b. The results after applying the filter on all three networks are shown in Figures 8b, 9b and 10b. As a result of filtration, the networks are not sustainable and trustable anymore due to a lack of trusted member and their interconnections.

Average degree is the measure of connectivity of nodes among themselves. After filtration of the most trustworthy nodes from all three networks, the average degree has been reduced greatly for all three networks as shown in Tables 3–5. Moreover, after filtration of the nodes given in Table 2, there is an increase in the network diameter and path length. As the degree of the filtered network was decreased, many links existing in the network disappear. Therefore, these links contained hubs (nodes with a lot of edges). After the dismissal of the hubs, the path becomes larger because the nodes having lower connectivity now require additional searching and hence require a higher number of hops. Further, there is a decrease in the clustering coefficient value for all three networks as demonstrated in Tables 3–5 because of the reduced degree of connectivity among the nodes caused by the smaller value of average degree centrality.

Table 3. The comparison of parameters before and after the filtration for the Facebook network.

Parameters	Before Filtration	After Filtration
Nodes	4039	1466
Edges	88,234	13,266
Average Degree	21.846	9.049
Average path length	3.693	5.581
Average clustering coefficient	0.617	0.616
Network Diameter	8	16

Table 4. The comparison of parameters before and after the filtration for the Twitter network.

Parameters	Before Filtration	After Filtration
Nodes	465,107	418,670
Edges	834,797	210,784
Average Degree	1.795	0.503
Average path length	6.919	7.017
Average clustering coefficient	0.01	0.005
Network Diameter	19	20

Table 5. The comparison of parameters before and after the filtration for the Slashdot network.

Parameters	Before Filtration	After Filtration
Nodes	82,168	35,597
Edges	948,464	45,102
Average Degree	11.543	1.267
Average path length	11.281	13.565
Average clustering coefficient	0.511	0.216
Network Diameter	13	17

Among the considered social networks in this study, the results demonstrate that Twitter is the most sustained network as it is still very famous among the people around the globe. Furthermore, it has high social capital as compare to the other network used for the experimentation. Facebook is found to be the least stable network as per the experiments conducted in this research. It is due to the least social capital and removal of nodes left a high influence on the sustainability of the network. Further, we must not ignore that this work just explains one particular social background, which is trust. We understand, though, that people come into many situations in their daily lives and that there is huge interdependence between contexts. Social networks may be analyzed based on different contexts and there is a change in the ego-network of an individual when the user undergoes some life-changing events. These events may include entering college or university for higher education, change of workplace, the adaptation of new hobby, moving to another city, getting married, etc. [57]. The social networks are geographically distributed around these contexts.

There are multiple factors for the collapse of social networks. One of the main factors is the induction of new and famous social media applications which attract the users and activity of the user on old social network decreases. The offered social capital in the new social media platforms might be the source of attraction for the shift of users from the old social networks. Although the analysis is based on the entire set of connections available, still we lack some constraints which are information about the parallel use of other social networks and the strength of ties.

6. Conclusions

Smart city solutions are a big challenge and their level of adaptation depends on the citizens' trust in the provided security. Bringing smart city into the SIoT world is a normal step but SIoT based security depends on multiple factors as SIoT is a paradigm involving IoT objects and their social

interaction with both humans and machines. The use of OSN by citizens is of significant importance, as the data of OSN can be used to know about the citizens' sentiments/opinions. We propose that the citizens' data posted on OSN can be used to introduce new services to smart cities. Further, the deployment of local and global trust mitigates the mixing of fake data. Furthermore, work is done to identify the sustainable OSN that can be used to know the opinion of people within a smart city.

There is not a single constraint behind the decay of any OSN, multiple mechanisms are responsible for the deterioration of the OSN. The gradual decay of many OSN is due to the rapid day by day development in the information technology infrastructure and induction of more attractive, user-friendly, and fascinating SIoT networking platforms. Many users shift to new OSN as well as stay on the old network simultaneously for a long time to establish a link to a separate network for their contacts. The shifting of the users from the old network to the new one is due to the user's preferences towards the network and results in the gradual decay of the old social network.

We analyzed three types of social networks by deploying our model. The objective of the analyses was to validate the model based on local and global trust factors. In addition, the proposed model is used to study the sustainability issue of social networks. Filteration of the most trusted users from the networks results in the reduction of a significant amount of nodes. After deploying the filters on Facebook, Twitter, and Slashdot social networks, only 36.3%, 90.03%, and 43.32% nodes respectively sustain in the network. From our results, it is seen that Twitter is the most sustained and Facebook is the least. Because, after filtration of local and global trusted users, the Facebook network is left with only 36.3% nodes and 90.03% nodes in the case of Twitter. Further, the results from the study of Facebook, Twitter, and the Slashdot network could not be generalized to other local or global OSN. The reason is that every social network has its own aspect and we cannot surely say about a social network's sustainability based on the other.

The extension of this research work may be claimed by taking into account other radical shifts in the OSN. The information that a user is a member of more than one social network could be used for further investigation. In addition, we need to do some work on deciding that when an online social community becomes the trusted community. A threshold value of the trust has to be defined for the community to be a trusted community.

Author Contributions: Formal analysis, A.U.R.; methodology, A.U.R.; conceptulization, D.H.; project administration, A.P. and D.H.; writing—original draft preparation, A.U.R.; writing—review and editing, A.U.R., R.A.N., M.T.S., and A.R.; supervision, A.P. and D.H.; funding acquisition, D.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported in part by the National Nature Science Foundation of China under grants 61471157, 61772090, and 61801055, in part by the Fundamental Research Funds for the Central Universities under grant 2018B23014, and in part by a National Research Foundation of Korea (NRF) grant funded by the Korean government (NRF-2017R1C1B5017464).

Acknowledgments: This work would not have been possible without the financial support provided by the Korea Institute for Advanced Study. We are especially thankful to Dildar Hussain for the conceptualization, funding acquisition, project administration, and supervision.

Conflicts of Interest: The authors claim that there are no conflicts of interest involved in publishing this article.

References

1. Atzori, L.; Iera, A.; Morabito, G.; Nitti, M. The social internet of things (SIoT)—When social networks meet the internet of things: Concept, architecture and network characterization. *Comput. Netw.* **2012**, *56*, 3594–3608. [CrossRef]
2. Fire, M.; Kagan, D.; Elyashar, A.; Elovici, Y. Friend or foe? Fake profile identification in online social networks. *Soc. Netw. Anal. Min.* **2014**, *4*, 1–23. [CrossRef]
3. Lőrincz, L.; Koltai, J.; Győr, A.F.; Takács, K. Collapse of an online social network: Burning social capital to create it? *Soc. Netw.* **2019**, *57*, 43–53. [CrossRef]
4. Fire, M.; Goldschmidt, R.; Elovici, Y. Online social networks: Threats and solutions. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 2019–2036. [CrossRef]

5. Gómez, V.; Kaltenbrunner, A.; López, V. Statistical analysis of the social network and discussion threads in Slashdot. In Proceedings of the 17th international conference on World Wide Web, Beijing, China, 21–25 April 2008; pp. 645–654.
6. Lampe, C.A.C.; Johnston, E.; Resnick, P. Follow the reader: Filtering comments on slashdot. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 27 April–3 May 2007; pp. 1253–1262.
7. Cherepnalkoski, D.; Karpf, A.; Mozetič, I.; Grčar, M. Cohesion and coalition formation in the european parliament: Roll-call votes and twitter activities. *PLoS ONE* **2016**, *11*, e0166586. [CrossRef]
8. Can, U.; Alatas, B. Big social network data and sustainable economic development. *Sustainability* **2017**, *9*, 2027. [CrossRef]
9. Rehman, A.U.; Jiang, A.; Rehman, A.; Paul, A.; din, S.; Sadiq, M.T. Identification and role of opinion leaders in information diffusion for online discussion network. *J. Ambient Intell. Humaniz. Comput.* **2020**, 1–13. [CrossRef]
10. Jagatic, T.N.; Johnson, N.A.; Jakobsson, M.; Menczer, F. Social phishing. *Commun. ACM* **2007**, *50*, 94–100. [CrossRef]
11. Koutrika, G.; Effendi, F.A.; Gyöngyi, Z.; Heymann, P.; Garcia-Molina, H. Combating spam in tagging systems. In Proceedings of the 3rd International Workshop on Adversarial Information Retrieval on the Web, Banff, AB, Canada, 8 May 2007; Volume 215, pp. 57–64.
12. Du, W.; Lin, H.; Sun, J.; Yu, B.; Yang, H. A new trust model for online social networks. In Proceedings of the 2016 1st IEEE International Conference on Computer Communication and the Internet, ICCCI 2016, Wuhan, China, 13–15 October 2016; pp. 300–304.
13. Rababah, O.; Alqudah, B. Building a Trust Model for Social Network. *Mod. Appl. Sci.* **2018**, *12*, 69. [CrossRef]
14. Caverlee, J.; Liu, L.; Webb, S. The SocialTrust framework for trusted social information management: Architecture and algorithms. *Inf. Sci.* **2010**, *180*, 95–112. [CrossRef]
15. Nepal, S.; Sherchan, W.; Paris, C. Building trust communities using social trust. In *International Conference on User Modeling, Adaptation, and Personalization*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 243–255.
16. Zhao, J.; Zhu, C.; Peng, Z.; Xu, X.; Liu, Y. User Willingness toward Knowledge Sharing in Social Networks. *Sustainability* **2018**, *10*, 4680. [CrossRef]
17. Mora, H.; Pérez-delHoyo, R.; Paredes-Pérez, J.F.; Mollá-Sirvent, R.A. Analysis of social networking service data for smart urban planning. *Sustainability* **2018**, *10*, 4732. [CrossRef]
18. Atzori, L.; Iera, A.; Morabito, G. From "smart objects" to "social objects": The next evolutionary step of the internet of things. *IEEE Commun. Mag.* **2014**, *52*, 97–105. [CrossRef]
19. Smith, K. 126 Amazing Social Media Statistics and Facts. Brandwatch Blog. Available online: https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/ (accessed on 1 March 2020).
20. Cavazza, F. Social Media Landscape. 2017. Available online: https://fredcavazza.net/2017/04/19/social-media-landscape-2017/ (accessed on 1 March 2020).
21. Butler, B.S. Membership Size, Communication Activity, and Sustainability: A Resource-Based Model of Online Social Structures. *Inf. Syst. Res.* **2001**, *12*, 346–362. [CrossRef]
22. Bharadwaj, K.K.; Al-Shamri, M.Y.H. Fuzzy computational models for trust and reputation systems. *Electron. Commer. Res. Appl.* **2009**, *8*, 37–47. [CrossRef]
23. Tang, J.; Gao, H.; Hu, X.; Liu, H. Exploiting homophily effect for trust prediction. In Proceedings of the 6th ACM International Conference on Web Search and Data Mining (WSDM 2013), Rome, Italy, 4–8 February 2013; pp. 53–62.
24. Fotia, L.; Messina, F.; Rosaci, D.; Sarné, G.M.L. Using local trust for forming cohesive social structures in virtual communities. *Comput. J.* **2017**, *60*, 1717–1727. [CrossRef]
25. Tang, J.; Hu, X.; Gao, H.; Liu, H. Exploiting local and global social context for recommendation. In Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence, Beijing, China, 3–9 August 2013; pp. 2712–2718.
26. The Statista Portal, Global Social Media Ranking 2020, Ranked by Number of Active Users (in Millions). Available online: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (accessed on 30 January 2020).
27. Mui, L.; Mohtashemi, M. A Computational Model of Trust and Reputation. In Proceedings of the 35th Hawaii International Conference on System Sciences, Big Island, HI, USA, 10 January 2002; pp. 188–196.

28. Ziegler, C.N.; Lausen, G. Propagation models for trust and distrust in social networks. *Inf. Syst. Front.* **2005**, *7*, 337–358. [CrossRef]
29. Celis, L.E.; Mousavifar, A.S. A Model for Social Network Formation: Efficiency, Stability and Dynamics. *arXiv* **2015**, arXiv:1510.09025.
30. Atzori, L.; Iera, A.; Morabito, G. SIoT: Giving a social structure to the internet of things. *IEEE Commun. Lett.* **2011**, *15*, 1193–1195. [CrossRef]
31. Grandison, T.; Sloman, M. A survey of trust in internet applications. *IEEE Commun. Surv. Tutor.* **2009**, *3*, 2–16. [CrossRef]
32. UNDESA. The World's Cities in 2016. Available online: http://www.un.org/en/development/desa/population/publications/pdf/urbanization/the_worlds_cities_in_2016_data_booklet.pdf (accessed on 25 February 2020).
33. Liu, S.M.; Yuan, Q. The Evolution of Information and Communication Technology in Public Administration. *Public Adm. Dev.* **2015**, *35*, 140–151. [CrossRef]
34. Ilieva, R.T.; McPhearson, T. Social-media data for urban sustainability. *Nat. Sustain.* **2018**, *1*, 553–565. [CrossRef]
35. Poletti, C.; Michieli, M. Smart cities, social media platforms and security: Online content regulation as a site of controversy and conflict. *City Territ. Archit.* **2018**, *5*, 1–14. [CrossRef]
36. Ballestar, M.T.; Cuerdo-Mir, M.; Freire-Rubio, M.T. The Concept of Sustainability on Social Media: A Social Listening Approach. *Sustainability* **2020**, *12*, 2122. [CrossRef]
37. Tse, R.; Zhang, L.F.; Lei, P.; Pau, G. Social Network Based Crowd Sensing for Intelligent Transportation and Climate Applications. *Mob. Netw. Appl.* **2018**, *23*, 177–183. [CrossRef]
38. Maheswaran, M.; Hon, C.T.; Ghunaim, A. Towards a gravity-based trust model for social networking systems. In Proceedings of the 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), Washington, DC, USA, 22–29 June 2007.
39. Huang, F. Building Social Trust: A Human-Capital Approach. *J. Inst. Theor. Econ.* **2007**, *163*, 552–573. [CrossRef]
40. Molm, L.D.; Takahashi, N.; Peterson, G. Risk and trust in social exchange: An experimental test of a classical proposition. *Am. J. Sociol.* **2000**, *105*, 1396–1427. [CrossRef]
41. Cook, K.S.; Yamagishi, T.; Cheshire, C.; Cooper, R.; Matsuda, M.; Mashima, R. Trust building via risk taking: A cross-societal experiment. *Soc. Psychol. Q.* **2005**, *68*, 121–142. [CrossRef]
42. Rehman, A.U.; Jiang, A.; Rehman, A.; Paul, A. Weighted Based Trustworthiness Ranking in Social Internet of Things by using Soft Set Theory. In Proceedings of the 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 6–9 December 2019; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2020; pp. 1644–1648.
43. Golbeck, J. Combining provenance with trust in social networks for Semantic Web content filtering. In Proceedings of the International Provenance and Annotation Workshop, London, UK, 9–10 July 2018.
44. Abdelghani, W.; Zayani, C.A.; Amous, I.; Sèdes, F. Trust Management in Social Internet of Things: A Survey. In *Conference on e-Business, e-Services and e-Society*; Springer: Cham, Switzerland, 2016; Volume 9844, pp. 430–441.
45. ITU-T FG-SSC. Overview of Key Performance Indicators in Smart Sustainable Cities. 2014. Available online: https://www.itu.int/en/itu-t/focusgroups/ssc/documents/approved_deliverables/tr-overview-ssc.docx (accessed on 27 February 2020).
46. Moustaka, V.; Vakali, A.; Anthopoulos, L.G. A systematic review for smart city data analytics. *ACM Comput. Surv.* **2019**, *51*, 1–41. [CrossRef]
47. Leskovec, J.; Lang, K.J.; Dasgupta, A.; Mahoney, M.W. Community Structure in Large Networks: Natural Cluster Sizes and the Absence of Large Well-Defined Clusters. *Internet Math.* **2008**, *6*, 29–123. [CrossRef]
48. Choudhury, M.; Lin, Y.-R.; Sundaram, H.; Candan, K.S.; Xie, L.; Kelliher, A. How Does the Data Sampling Strategy Impact the Discovery of Information Diffusion in Social Media? In Proceedings of the ICWSM, Washington, DC, USA, 23–26 May 2010; pp. 34–41.
49. McAuley, J.; Leskovec, J. Learning to discover social circles in ego networks. *Adv. Neural Inf. Process. Syst.* **2012**, *1*, 539–547.
50. Abdul, R.; Paul, A.; Gul, M.J.; Hong, W.H.; Seo, H. Exploiting small world problems in a SIoT environment. *Energies* **2018**, *11*, 2089. [CrossRef]
51. Adalat, M.; Niazi, M.A.; Vasilakos, A.V. Variations in power of opinion leaders in online communication networks. *R. Soc. Open Sci.* **2018**, *5*, 180642. [CrossRef] [PubMed]

52. Bastian, M.; Heymann, S. Gephi: An Open Source Software for Exploring and Manipulating Networks. In Proceedings of the Third International Conference on Weblogs and Social Media, San Jose, CA, USA, 17–20 May 2009; AAAI Press: Menlo Park, CA, USA, 2009; pp. 361–362.
53. Cherven, K. *Mastering Gephi Network Visualization*; Packt Publishing Ltd.: Birmingham, UK, 2015; ISBN 9781783987344.
54. Yifan, H. Efficient, High-Quality Force-Directed Graph Drawing. *Math. J.* **2005**, *10*, 37–71.
55. Jacomy, M.; Venturini, T.; Heymann, S.; Bastian, M. ForceAtlas2, a continuous graph layout algorithm for handy network visualization designed for the Gephi software. *PLoS ONE* **2014**, *9*, e98679. [CrossRef]
56. Feng, Y. Are you connected? Evaluating information cascades in online discussion about the #RaceTogether campaign. *Comput. Hum. Behav.* **2016**, *54*, 43–53.
57. Brooks, B.; Hogan, B.; Ellison, N.; Lampe, C.; Vitak, J. Assessing structural correlates to social capital in Facebook ego networks. *Soc. Netw.* **2014**, *38*, 1–15. [CrossRef]