ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

A Strategy of Trust Management in Social Internet of Things community

Dr. K. Praveen Kumar

Associate Professor, Department of Computing, School of Electrical Engineering & Computing, Adama Science &Technology University, Adama, Ethiopia

ABSTRACT:A social Internet of Things (IoT) framework can be seen as a blend of traditional disbursed systemsand informal communities, wherein "matters" self-sufficiently set up social connections as in keeping with the proprietors' interpersonal groups, and look for relied on "matters" which could supply administrations required whilst they arrive into touch with each different deftly. A new search for of the proper item that could offer the desired provider. A newparadigm known as Social Internet of Things has been introduced and proposes the integration of social networkingstandards into the Internet of Things. The beneath idea is that every item can search for the favoured provider the use of itsfriendships, in a allotted way. The cluster among Internet of Things (IoT) and social networks (SNs) allows the relationship of human beings to the ever-present computing universe.

KEYWORDS: Internet of things, social networks, SIOT, trustworthinessmanagement

I. INTRODUCTION

The Internet of things is the network of interrelated electronic sensor devices that gather data, communicate with each other, and can be supervised remotely over the internet. The goal of the IOT's development is to connect the environment and physical world to the wireless networks; this would allow making machines, objects and work environments interactive. By using IOT sensors, objects will be capable of interchanging the data with other machines without the help of human interference. The IOT includes various technology devices, infrastructure and services such as the computing, cloud computing, data analytics and mobile. The internet of things is a sensible and valid trend that is moving ahead and rapidly. There are main platforms and discoveries that have had a rich remuneration of complexity, global reach and novelty. But the IOT is for certain a trend that takes the growing of interlink to another level. There will be a mammoth range of interlinked systems and products that the IOT will enable, from elementary surveying of room temperature and security to the measure self to fully networked factories and hospitals, to automated cities. While it is genuine that the IOT will intend a major shift in the politics, economy and regulations from all government agencies, companies and non-profit organizations, here will mainly focus on the effects that it will have on citizens by arguing that, although the development of the IOT is still on early stages involving its development and spread, it is potentially a threat to both security and privacy.

Since the IOT is a growing trend, most major companies are searching to get implied, there are tremendous efforts to trigger this trend as something positive in the upcoming future. An often converse that is present in the media named the major positivetechnological betterment that the IOT represents. Lot of devices connected to the internet gather valuable personal data from users,such as name address, date of birth, credit card numbers and health data. The study bring out that all this data is vulnerable topotential hacker attacks. If the data that is stored in the interlinked devices stand for threat to consumer's safety and privacy, whathappens when this data relies on other companies' hands is a threat as well. Insurance companies have encompass with joy the reachof the IOT, claiming that they could produce ways to collect information related to health behaviour and built to design their rateoblations. Devices that calculate physical activity, blood pressure, blood sugar, weight and other health based metrics could furnishuseful health information about individuals to insurance companies. The fact that the base endures the internet-connected devices isundependable and can fail exhibit a disadvantage to the IOT as well. The infrastructure that endorses the internet

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

works otherwiseacross diverse geographical areas. The monopoly has the company that supply internet to users and companies. It is too expensive,undependable and it fails often. Users can spend hours or days without internet and support team is not effective and volatile.

Furthermore alteration in the infrastructure and weather conditions persist as an obstacle to objects connected to the internet. Inconclusion, there is the environmental wallop that the development and distribute the global IOT will bring. The Internet of thingswill be here sooner rather than later, for now it is a trend that is running fast to become a reality. Under this fact it is essential thatwe demand public access to technological knowledge about the IoT. Technology moves quicker than the development of suitablelegal valuate and action to modulate it. The IOT is something that will not damage our privacy and safety.Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices. Current market examples include smart thermostat systems and washer/dryers that utilize Wi-Fi for remote monitoring.

II. RELATED WORK

SIoT idea is sooner or later formalized in a few methods,primarily bases at the concept that items in IoT belong to peoplewithin the network [6, 7] and people offer services via theirowned gadgets. SIoT, as a result, is taken into consideration as social networks inwhich any tool is able to establishing socialrelationships with others in line with its proprietors. Theseentities expose their characteristics to public regions vianow not simplest themselves however also the proprietors' behaviors.Among several SIoT models proposed, we keep in mind theSIoT environment advanced via Atzori et al. [6]; and theacronym SIoT we use on this paper refers to this model. InSIoT, every tool has one or extra proprietors who may alsohave a few other devices. The version applies some predefined regulations and mechanisms by using utilizing the socialrelationships amongst human beings in truth. For example, everyconsumer in SIoT continues its social courting by means of consideringthe term "buddies". If two customers are "friends", then the devicesthey owned tend to be cooperative with every different. The time period"network-interest" is taken into account because theenvironment in which gadgets are tent to be carried oroperated (e.g. Workplace, home, paintings place, public/social locations).

As a consequence, gadgets in comparable groups probableproportion their data each other. These entity in SIoT areexpected to talk through overlay social communityprotocols, or underlying widespread tool-to-tool communication network protocols like Machine-to-Machine(M2M) or P2P, forming an social network of gadgets that's capability for the SIoT. As a end result, types of socializationamongst objects are foreseen; and sorts of social relationshipsare also hooked up [6, 7] as illustrated in Fig.1.

According to the SIoT version, our proposed believe providerplatform is capable of instantiate a collaborative surroundings,allowing entities to share their trust associated statistics, asprecipitated from their know-how and enjoy, by means of filingtheir critiques to a recognition machine.

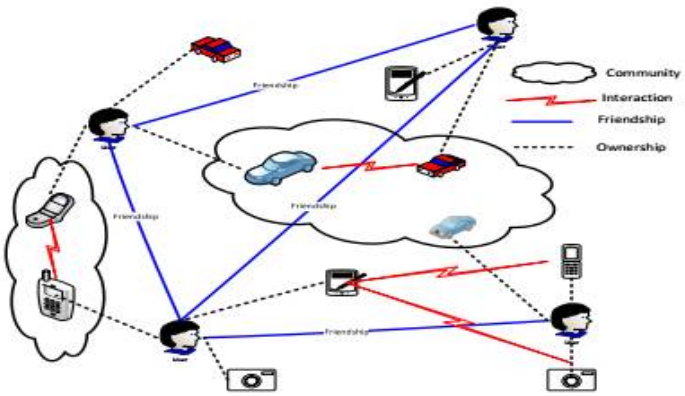

Fig. 1. Social structures of the Internet of Things

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

There are diverse types of agree with definitions main toproblems in organizing a not unusual, widespread notation thatholds, regardless of personal dispositions or differingsituations. Generally, consider is taken into consideration as a computationalvalue depicted through a relationship between trustor and trustee,described in a selected context and measured by way of believe metricsand evaluated by using a mechanism. Some essential homes ofagree with are stated and mentioned. Previous studieshas shown that accept as true with is the interplay amongst human, socialsciences and pc science, suffering from numerous subjectivefactors which includes social fame and bodily homes; andgoal factors together with competence and reputation. Thecompetence is size of abilities of the trustee toperform a given mission that's derived from trustee's diplomas,certifications and enjoy. Reputation is shaped by way of theopinion of other entities, deriving from 1/3 events' evaluationsof previous interactions with the trustee.

A consider machine covers a huge range of trust-relatedresearch factors ranging from Trust Relationship andDecision (TRD), Data Perception Trust (DPT) to IdentityTrust (IT). Several works awareness on agree with evaluation andconsider assessment in IoT and in SIoT [13]. The authorsanticipate that entities inside the structures are human-related orhuman-carried which are capable of organizing family membersrelying and cooperatively running collectively accordingwith their owners' relationships. They proposed distributed,stumble upon-based totally, and activity-based trust controlprotocols wherein entities compute and replacetrustworthiness of the companions once mutual interactions arise.The entities additionally proportion agrees with evaluations to their friends asrecommendations to help friends of their trust-associatedtactics. Thus, a reputation-based totally mechanism is needed toincorporate with the believe structures. However, maliciousentities (cheating or socially uncooperative entities) may want toexploit the main recognition-primarily based residences to interrupt thefunctionalities of the gadget the usage of trust-associated assaults along with self-promoting, ballot -stuffing, discriminatory, badmouthing, precise-mouthing, and whitewashing.

III.PROPOSED SYSTEM

Humans usually interact with others in a wide variety ofrelationships during their everyday life. Also, they wouldutilize many smart services and applications from IoTimprove their life quality. In IoT, as mentioned above, anindividual user connects to the other(s) via legacy networks;on the other hand, sets of things collaborate with each othervia the Internet for offering information to smart services andapplications, while each user uses them. In order to practicallyintegrate the ubiquitous computing in our future daily lifewith high Quality of Experience (QoE), we need to improvethe connectivity of all the relationships between users andthings, and to enhance the availability of computational powervia sets of things surrounding us. [2] Therefore, we takeinto consideration social networks (SNs) of all entities(i.e., humans and things) for ubiquitous computing as anevolution beyond the IoT. In other words, things should besocialized for allowing humans to establish relationships withthem in an easy way.

For this objective, there are twoconsiderations as shown in Fig. 2:
1) Increasing sociality (or connectivity) and
2) Improving pervasiveness (or availability)

In this section we provide an overview of a possibleimplementation of the SIoT. Here the major functionsrequired to run the SIoT are illustrated. To describe theproposed system we resort on the simple three-layerarchitectural model for IoT presented in. [1] it consists of:

i. The sensing layer, which is devoted to the data, acquisition and node collaboration in short- rangeand local networks;
ii. The network layer, which is aimed at transferringdata across different networks; and
iii. The application layer, where the IoT applicationsare deployed together with the middlewarefunctionalities.
Figure 2 shows the resulting three-layer architecture. Thethree basic elements of the proposed system are: the SIoTServer, the Gateway, and the Object.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

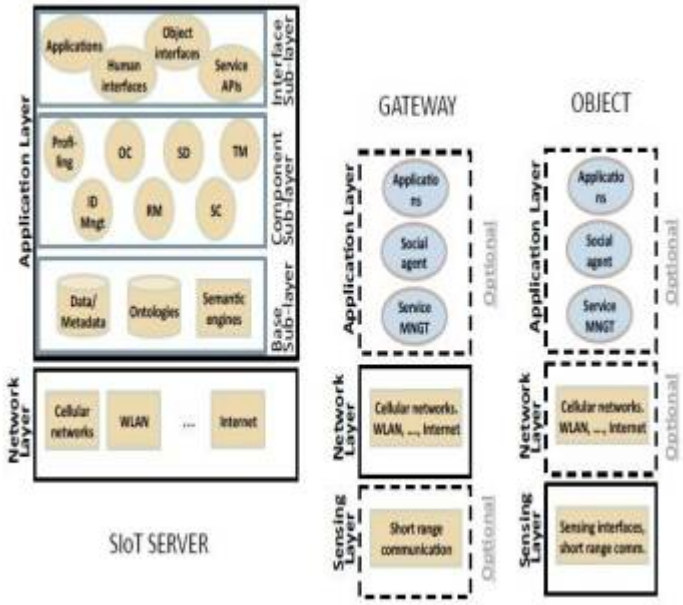

Fig.2: System architecture

Following the three- layer model made of the sensing,network, and application layer. The main SIoT componentsbelongs to the application layer, wherein the relationshipmanagement (RM), service discovery (SD), servicecomposition (SC), and trustworthiness management (TM)functionalities are located. The lines represent the optional
layers in both the object and the gateway architecture.[1]

The basic elements of SIoT are: Application Layer
i) Base sub-layer: Includes the database for the storage and themanagement of the data and the relevant descriptors. Recordthe social member profiles and their relationships. Record theactivities carried out by the objects in the real and virtualworlds. Data about humans (object owners as well as visitors)are also managed.

ii) Component sub-layer: Includes the tools that implementthe core functionality of the SIoT system. ID management assigns an ID that universally identifies all the possiblecategories of objects. Profiling configures manually andautomatically a (static or dynamic) information about theobjects.

a) Owner control (OC) define activities performedobject, information that can be shared, set of objectswhich can access such information and type ofrelationships that can be setup.
b) Relationship management (RM) allow objects tostart, update, and terminate their relationships withother objects.
c) Service discovery (SD) finds which objects canprovide the required service.
d) Trustworthiness management (TM) defines howthe information provided by the other members shallbe processed.
e) The service composition (SC) component enablesthe interaction between objects. Most of the time,the interaction is related to an object that wisheseither to retrieve an information about the real worldor to find a specific service provided by anotherobject.
iii) Interface sub-layer: Here the third-part interfaces toobjects, humans, and services are located. This sub-layer maybe mapped onto a single site. It can be deployed in a federatedway by different sites, or deployed in a cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 8, August 2016

IV. CONCLUSION

The Social Internet of Things could berealized faster than the average user would think. Mostof the essential technological advances desirable for it havealready been made but its impact on the legal, moral, securityand social fields would delay the implementation. Efforts aremade to overcome these challenges. Study has been performedhere on the methods to improve the security in SIoT byimplementing the different phenomena to compute thetrustworthiness factor.

REFERENCES

[1] Luigi Atzori*, Antonio Iera**, Giacomo Morabito***,and Michele Nitti: The Social Internet of Things(SIoT) - When Social Networks meet the Internet ofThings: Concept: Architecture and NetworkCharacterizationI: Paper submitted and published inComputer Networks, Volume 56, Issue 16,14 November2012, Pages 3594–3608.
[2] Michele Nitti, Roberto Girau, and Luigi Atzori,SeniorMember,IEEE Trustworthiness Management in theSocial Internet of Things: IEEE TRANSACTIONS ONKNOWLEDGE AND DATA ENGINEERING, VOL.26, NO. 5, MAY 2014
[3] Antonio M. Ortiz, Member, IEEE, Dina Hussein,Soochang Park, Member, IEEE, Son N. Han,Student Member, IEEE, and Noel Crespi, SeniorMember, IEEE.Cluster Between Internet of Thingsand Social Networks: Review and ResearchChallenges :IEEE INTERNET OF THINGS JOURNAL, VOL. 1,NO. 3, JUNE2014
[4] Kazi Masudul Alam_, Mukesh Sainiy, and AbdulmotalebEl Saddik; Multimedia Computing Research Laboratory,
University of Ottawa, Ottawa, ON, Canada; Division ofEngineering, New York University, Abu Dhabi,UAETowards Social Internet of Vehicles: Concept,Architecture and Applications:DOI10.1109/ACCESS.2015.2416657, IEEE Access
[5] Michele Nitti*, Luigi Atzori*, Irena Pletikosa Cvijikj;University of Cagliari, Italy, michele.nitti,l.atzori@diee.unica.it ETH Zurich, Switzerland,ipletikosa@ethz.chFriendship selection in the SocialInternet of Things: challenges and possible strategies;DOI10.1109/JIOT.2014.2384734, IEEE Internet ofThings Journal
[6] Google Images on Internet of Things and Social InternetofThings.
[7] Wikipedia on Social Internet of Things and InternetofThings.
[8] L. Atzori, A. Iera, and G. Morabito, "The Internetof things: A survey," Comput. Netw., vol. 54, no. 15, pp.2787–2805, 2010.
[9] P. Mendes, "Social-driven Internet of connected objects,"in Proc. Interconn. Smart Objects with the InternetWorkshop, Lisbon, Portugal, 2011.
[10] L. Ding, P. Shi, and B. Liu, "The clustering of Internet,Internet of things and social network," in Proc. 3rd Int.Symp. KAM, Wuhan, China, 2010.
[11] D. Guinard, M. Fischer, and V. Trifa, "Sharing usingsocial networks in a composable web of things," in Proc.8th IEEE Int. Conf. PERCOM Workshops, Mannheim,Germany,2010.
[12] E. A. K. amd, N. D. Tselikas, and A. C. Boucouvalas,"Integrating RFIDs and smart objects into a unifiedInternet of things architecture," Adv. Internet Things,vol. 1, no. 1, pp. 5–12, 2011.
[13] L. Atzori, A. Iera, and G. Morabito, "SIoT: Giving asocial structure to the Internet of things," IEEECommun. Lett., vol. 15, no. 11, pp. 1193–1195, Nov.2011.
[14] J. Surowiecki, the Wisdom of Crowds, New York, NY,USA: Doubleday, 2004. [8] R. Roman, P. Najera,and J. Lopez, "Securing the Internet of things,"Computer, vol. 44, no. 9, pp. 51–58, 2011.
[15] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito,"A subjective model for trustworthiness evaluation inthe social Internet of things," in Proc.IEEE 23rd Int.Symp. PIMRC, Sydney, NSW, Australia, 2012, pp. 18–23

BIOGRAPHY

Dr.K.Praveen Kumar received the PhD in Computer Science & Engineering in 2015, M.Tech in Software Engineering from Kakatiya Institute of Technology & Science Warangal, Telangana, India in 2010 and B.Tech in Information Technology from Kakatiya Institute of Technology & Science Warangal, Telangana, India 2007. Presently working as Assistant Professor in Computer Science Department at Adama Science and Technology University, Adama, Ethiopia.