Challenges in Iot with Basic Algorithm for Friend Selection

Prajwal S. Gaikwad
AISSMSIOIT,Pune.

Minal A Zope
AISSMSIOIT,Pune.

ABSTRACT
Today's world deal with different technologies. Consider the devices used as things and try to from a network of these devices such that these use internet and from internet if it is possible to connect these devices so that they can interact with each other then the devices as things and the the networking of things as Internet of things. so a formal definition can be loT is the networking of everyday objects which interact to each other and also connected to the internet. Many smart applications which support and simplify everyday life can be enabled by the loT. Normally the things are connected by cloud. Due to special requirements, the design of loT module is very complex and is a great challenge in research. The loT system is required to connect large amount of things to the cloud system. Therefore an open API should also be provided for easy data access and interoperability. As a result, loT system can be accessed and controlled from anywhere and anytime using any device, one of which is Smartphone.

Keywords
IoT Systems,SIOT.

1 INTRODUCTION
Basic functionality of loT system is remote monitoring and controlling [1] [3] [4]. Based on this basic functions, many types of smart applications can be implemented.As variety of applications are there on smartphones so it can be said that IoT increases convenience ,provide better lifestyle, reduces expenses. If an openAPI is provided the business boundaries can be broadened. So businesses sell many products with less expences.

Many day to day applications[1] can be developed like smart house, smart energy, intelligent traffic system, as well as eHealth application. For example in eHealth application, loT system can monitor user blood pressure and heart rate, additionally it also tracks user's behavior and activities. Based on those data, loT smart system can suggest doctor's treatment plan, prescription etc.

Various applications[6][7][8][12] are shown in **Fig 1.**

Second application can be device tracking which can help in security purposes of vehicles on can be used for personal security also.

Another application can be home automation which is now becoming a basic need of today's world. In smart home we can have all the appliances connected so that we can control them remotely.A smart city can be developed with these self organizing and self configuring devices in the real world like we can have street lights that are controlled with the real time temperature and light controlling and sending devices.

Traffic control can be of greater help in the world of increasing traffic chaos, a real time devices to sense the traffic and controlling features can be added for a better city traffic control.

2 SYSTEM ARCHITECTURE
The loT system consists of cloud system and loT module.[1][2] The loT module consists of connectivity, data

processing unit and sensing or actuating module. The connectivity has a function to connect all loT module to the internet and cloud server. It consists of communication and networking module.So the device user is using comes under IoT module and the services provided to the IoT module are stored on cloud.

The basic block diagram is shown in **Fig 2.**

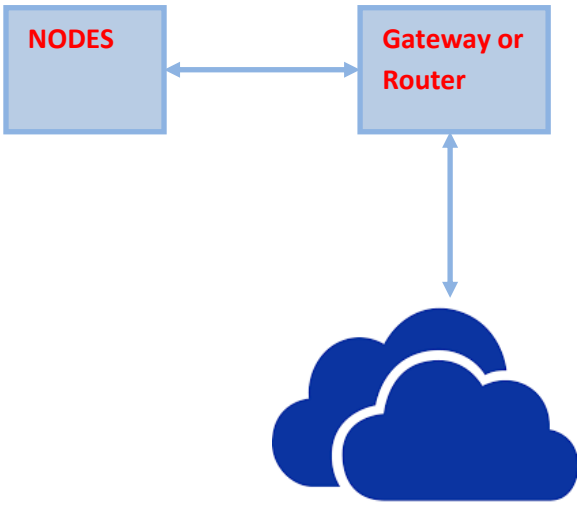

Fig 2: Basic Block Diagram

The nodes can be any smart device which is connected to the cloud by using a gateway or router.

3 BASICS OF IOT
IoT bridges the gap of physical and technical worlds as it is a combination of different technologies[3][4]. It have many capabilities which include:

− Communication and cooperation: Things network with Internet resources or even with each other with automatic configuration, to make use of data and services It also update it's state automatically. As to communicate with each other various network standards comes into picture like GSM, Wi-Fi, Bluetooth ,and ZigBee etc. Basically it is a heterogeneous network[13] system which is combination of wired as well as wireless systems connected through internet.

− Object Addressability: Within an Internet of Things, objects can be addressed with look-up or name services like that of DNS services. And as the objects are networked they can be located easily by using these services.

− Sensing: Objects or things uses sensors to collect information about their surroundings, record that information and pass it to other things or objects or else directly react to it.

− Actuation: Objects contain actuators to manipulate their environment. Real-world processes are controlled remotely with these actuators via the Internet.

− Object Identification: Objects are uniquely identifiable. The identification helps in linking to the information or data associated with that particular object. That information can be retrieved by the mediator which is connected to the server or cloud server. RFID or bar codes do not have built in energy resources so they can be called as passive objects ,with which the identification can be done.

− Embedded information processing: Smart objects have a processor or microcontroller,

plus storage capacity. These resources can be used, for example , to process and interpret sensor information, or to give products a "memory" of how they have been used.

− Localization: Smart things are built in capability to get their physical location, so can be located. Various technologies that are available are GPS or the mobile phone network , as well as ultrasound time measurements, UWB (Ultra-Wide Band), radio beacons (e.g. neighboring WLAN base stations or RFID readers with known coordinates) and optical technologies can be used for localization.

− User interfaces: Various interfaces are available to have communication between the objects and people for example the Smartphone are having user interface which is simple to use. Various method like speech recognition, gesture recognition are added capability to these Smartphone which add to the simplicity and flexibility in using the interface.

4 TECHNOLOGICAL CHALLENGES

Though the applications outlined above are very interesting but the demands for the technologies underlying it is very substantial[10]. Progressing from the Internet of computers to Internet of Things is something that must therefore be done one step at a time. There is a basic expectation that the technology must be available at low cost if a large number of objects are actually to be equipped, also there are many other challenges[2][3], such as:

− *Scalability:* The overall scope of Internet of Things is much more than that of Internet of computers because the number of devices or things is increasing day by day. SO scalability is the main technological challenge that need to be addressed .The things first cooperate between the local environment then to the global environment .So the communication and service discovery needs to be equally efficient in local as well as global environment. The objects that are added newly to the environment should not get affected by the number of networks connected.

− *Object operations:* Smart everyday objects or the mobile things should configure themselves to suit their environments unlike computers which are configured by the users.

− *Interoperability:* The things in IoT are of large number of varieties with need of different information ,different communication protocols used ,with varying capabilities. The operate at very different conditions like communication bandwidth, energy consumption etc and also the IP addressing in conventional internet domain. So interoperability is a major challenge in the heterogeneous environment and heterogeneous devices.

− *Software complexity:* Although the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems, a more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them.

-Data Volumes: As number of nodes is dynamic and most of the times it is increasing the volume of data is very large which is been transferred between the nodes

-Power supply: Due to heterogeneous nodes or devices the power supply need is varying .The passive devices like RFID do not need power supply but the need of power for active devices is a topic of concern and they rely on future services[11] which need less power supply or generate power themselves[5][6].

5 TRUST MANAGEMENT IN IOT WITH FRIENDS SELECTION

Due to openness and heterogeneous nature of the IoT it is very important that the data that is being transferred in Iot should have additional security measures than only the cryptography or access control mechanisms. An additional mechanism called as trust management[9] should be added . There can be many techniques to trust the network or node to which we are passing the data while using IoT.

We need a decision making algorithm for trust management. The basic algorithm for trust management can be as given in algorithm 1.

5.1 Algorithm 1

Algorithm Trust(DomainID)

{
$If(DomainID\ already\ in\ Registry)$
$Send\ the\ data\ and\ control\ information;$
}
$Else\{$
$Add\ an\ entry\ to\ the\ Registry;$
$TrustValue$
$= Check\begin{pmatrix}Send\ sample\ data\ to\ check\ for\ validity\\ of\ the\ user\ \ DomianIDReceiver\end{pmatrix}$
}
$If(Trustvalue == 1)$
{
$Add\ as\ a\ friend$
}
$Else$
{
$Add\ to\ Black-List$
}
}
Algorithm Check(Data, receiverID)
{
$Check\ in\ Neighbour's\ List;$
$If(Present\ in\ Trust\ registry)$
$Return\ 1;$
$Else$
$return\ 0;$
}

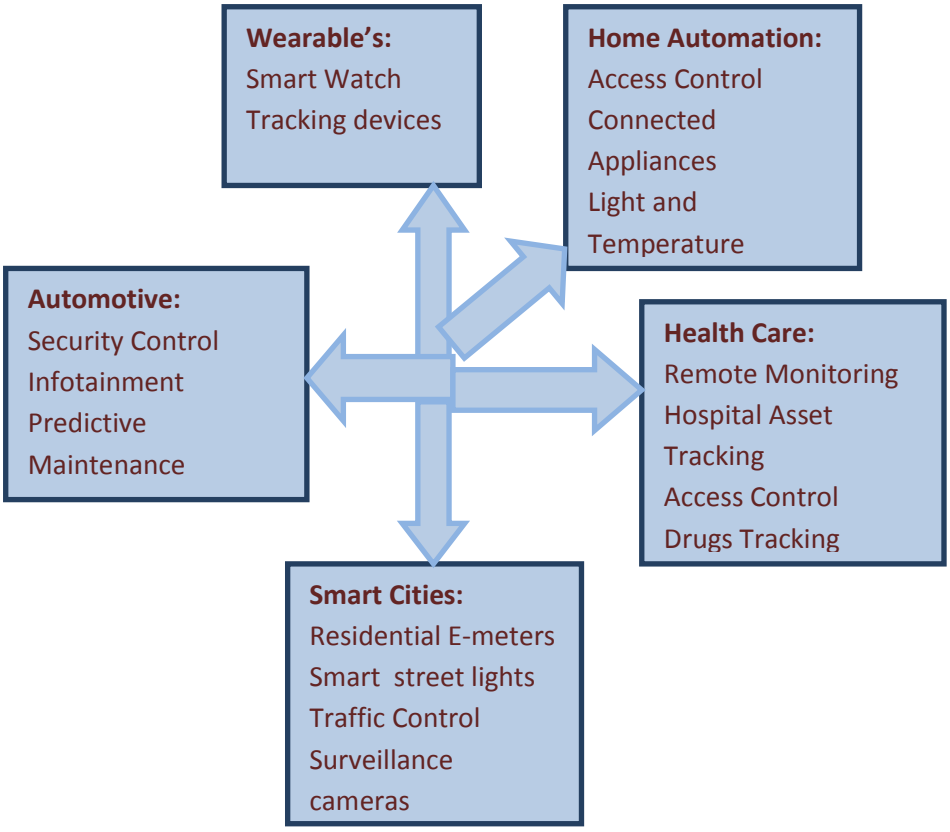

Fig 1:Applications of IoT

This simple algorithm checks the domainID or we can say the identity of the communicating machine and verify it's entry with the neighbors if it's trust value is 1 the entry is added to friend's registry or it is black listed. It can be removed from black list if it is found afterwards in the friend's entry of the neighbors. We can use a timestamp to verify the entries from blacklist after a period of time to crosscheck if they can be added to the friend's list or not.

There are a lot of functions to be added to the basic algorithm but the idea is to build a friend selection mechanism to IoT[2][3][4][5][6][14].

So with every service provider and requester a trust management needs to be added for the added security in IoT.As IoT is now used for social networking also we are referring that network as social IoT i.e SIOT[2][5][6]. For social networking sites various security measures are taken but for SIOT it needs to be combination of those technologies .Different routing algorithms are used to transfer data from one cloud to the other built for the security of that need to add the trust mechanism between the communicating peers or clouds. The need for trust is very clear ,there can be n number of misbehaving nodes which are passing malicious data for the own sake or for the damaging others data .Every time the data that is sent onto the network can not take the same path so the entries in the friends list is every time dynamic in nature it can not be fixed ,we have to add or remove entries in the list depending on the nature of route that the data follows. SO friend selection have a very important role in IoT or SIOT.

6 CONCLUSION

The basics of IoT are discussed so that it creates awareness of the mechanism and a brief overview of the security in IoT can be added with the basic algorithm which gives a view of friend selection in IoT.The future scope can be a trusted communication with the friend selection procedure incorporated with reduced time for communication path as a registry of trusted friends maintains the list of networks trusted maintained.

7 REFERENCES

[1] Luigi Atzori, Antonio lera, Giacomo Mo-rabito. The Internet of Things: A survey,Computer Networks, Volume 54, Issue 15, 2010, pp. 2787-2805.

[2] A IEEE INTERNET OF THINGS JOURNAL, VOL. 2,NO. 3, JUNE 2015 Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies Michele Nitti, Luigi Atzori, and Irena Pletikosa Cvijikj

[3] From the Internet of Computers to the Internet of Things Friedemann Mattern and Christian Floerkemeier Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich {mattern,floerkem}@inf.ethz.ch

[4] Mattern, F., Floerkemeier, C.: Vom Internet der Computer zum Internet der Dinge. Informatik-Spektrum 33(2):107–121 (2010)

[5] S Floerkemeier, C., Langheinrich, M., Fleisch, E. Mattern, F., Sarma, S.E.: (eds.) The Internet of things First International Conference, IOT 2008, LNCS 4952 Springer (2008)

[6] Frank C., Bolliger, P., Mattern, F., Kellerer, W.: The Sensor Internet at Work: Locating Everyday Items Using Mobile Phones. Pervasive and Mobile Computing (3):421–447 (2008)

[7] L Atzori, A. Iera, and G. Morabito, "From 'Smart Objects to'Social Objects': The Next Evolutionary Step of the internet of Things ," *IEEE Comm.*, vol. 52, no. 1, 2014, pp. 97–105

[8] A Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, ``Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22_32, Feb. 2014.

[9] Trust Management Mechanism for Internet of Things by GU Lizet, WANG JingpeP, SUN Bin

[10] 2014 1st International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE) Challenges and Opportunities in Designing Internet of Things by Trio Adiono

[11] Future Internet Assembly, "European Future Internet portal."[Online].Available: http://www.future-internet.eu/

[12] ABIresearch News. 2014. The Internet of Things Will Drive Wireless Connected Devices to 40.9 Billion in 2020 [Online]. Available: http:// Iwww.abiresearch.com/press/the-intern et –ofthings-will-drive-wireless-connect

[13] Improving Heterogeneous SOA-Based IoT Message Stability by Shortest Processing Time Scheduling, Jenq-Shiou Leu, Member, IEEE, Chi-Feng Chen, and Kun-Che Hsu IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 7, NO. 4, OCTOBER-DECEMBER 2014

[14] Building trust in the Human-Internet-of-Things Relationships IOANNIS KOUNELIS, GIANMARCO BALDINI, RICARDO NEISSE, GARY STERI, MARIACHIARA TALLACCHINI, AND ÂNGELA GUIMARÃES PEREIRA , IEEE TECHNOLOGY AND SOCIETY MAGAZINE | WINTER 2014 1932-4529/14