International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

# INTERNET OF THINGS AND TRUST MANAGEMENT IN IOT – REVIEW

**Neeraj[1], Amitpal Singh[2]**

[1]Student (M.tech), Department of Computer, Science and Engineering, Guru Nanak Dev University

Regional Campus, Gurdaspur, Punjab, India

[2]Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Dev University

Regional Campus, Gurdaspur, Punjab, India

---

**Abstract :** *The phrase Internet of Things (IOT) heralds a vision of the future Internet where connecting physical things, from bank notes to bicycles, through a network will let them take an active part in the Internet, exchanging information about themselves and their surroundings. This will give immediate access to information about the physical world and the objects in it—leading to innovative services and increase in efficiency and productivity. Trust management plays an important role in IOT for reliable data fusion and mining, qualified services with context-awareness, and enhanced user privacy and information security. This paper studies the state-of-the-art of trust management in IOT and presents, challenges, trust meaning, trust objectives.*

## 1. INTRODUCTION

The Internet of Things (IOT) involves the technology which links the objects of the real world to the virtual world with the help of unique identifiers and communicate each other through network, and enables anytime, anywhere connectivity of objects for anything that has an ON and OFF switch.

Internet of Things (IOT) provides an environment in which objects, animals or people are seems to be connected with the unique identifiers like chips and sensors with the ability to transfer data over a network without the involvement of human-to-human or human-to-computer interaction. Internet of Things specifies a general concept for the ability of large number of network devices to sense, collect and generate large amount of data from the world around us, and then share that data across the Internet where it can be sensed, processed, controlled and utilized for various useful purposes. Objects that are interconnected provides data regularly collected, analyzed and used to initiate any action, providing a wealth of intelligence for planning, management and decision making. IOT has evolved from the convergence of wireless technologies, like micro-electromechanical systems (MEMS) and the Internet.

### 1.1 What is thing in Internet of Things (IOT)?

In the Internet of Things, a thing can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors and chips to alert the driver when any obstacle comes in vehicle like when, route is wrong, tire pressure is low etc. Interconnected Objects can be natural or man-made that have uniquely addressable with assigned an IP address of 32-bit based on standard communication protocols and

must have ability to transfer data over a network to communicate around the world around us.[1].

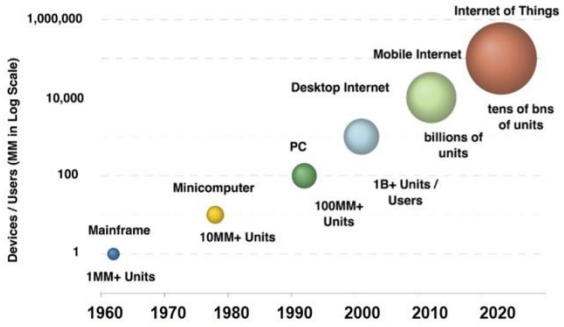
The Internet of Things (IOT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and will be able to uniquely identify themselves to other devices. In "Internet of Things" a "thing" could be Real/physical Entity Digital/virtual that exists and move in space and time and is capable of being identified. Examples of "things" include:

- Location (of objects)
- People
- Time Information (of objects)
- Condition (of objects)

These "things" of the real world shall seamlessly integrate into the virtual world, enabling anytime, anywhere connectivity [2].

Things are commonly identified either by assigned identification numbers, names and/or location addresses .The Internet of Things allows people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. [3].

In 2010, the number of everyday physical objects and devices connected to the Internet was around 12.5 billion. Cisco forecasts that this figure is expected to double to 25 billion in 2015 as the number of more smart devices per person increases, and to a further 50 billion by 2020.




### 1.2 Internet Of Things Demand:

- Complete understanding of any situation of its users and their appliances.
- Software architecture and pervasive communication networks for sensing, processing and conveying contextual information to where it is relevant and needed.
- Use of Standard Protocols for the security of information and data to be processed.
- Provides tools in IOT that aim for autonomous and smart behavior [3].

### 1.3 Challenges & Future Trends of IOT

The flow of data and work is analyzed in enterprise environment, office, home, and other smart spaces for future will be characterized across the organization interaction, requiring the operation of highly dynamic and ad-hoc relationships. At present, only a very limited ICT support is available, and the following key challenges exist.

**Network Foundation**: It specifies how to find network for connecting devices. Have limitations of the current Internet architecture in terms of, availability, manageability and scalability, mobility are some of the major barriers to IOT.

**Security**: In the domain of security the challenges are: Securing the architecture of IOT, security must be ensured

at design time and execution time and securing the IOT system from arbitrary attacks.

**Privacy:** In the domain of user privacy, the specific challenges are: Control over personal information (data privacy) and control over individual's physical location and movement (location privacy). Need for privacy enhancement technologies and relevant protection laws, and standards, methodologies and tools for identity management of users and objects.

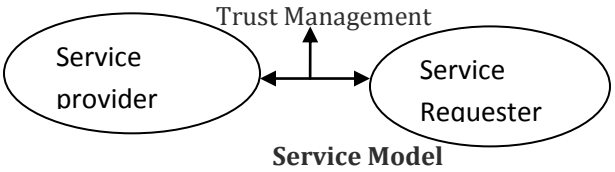
**Trust**: In the domain of trust, some of the specific challenges are: Need for easy and natural exchange of sensitive, protected and critical data e.g. smart objects will communicate on behalf of users / organizations with services they can trust. Trust has to be built in design part of IOT.

**Managing heterogeneity**: In the domain of Managing heterogeneity, some of the specific challenges are: Need for mange large amount of data to provide useful services, designing an efficient architecture for sensor networking and storage and mechanisms for sensor data discovery. Designing sensor data communication protocols, sensor data query, publish/subscribe mechanisms, developing sensor data stream processing mechanisms, and sensor data mining—correlation, design for aggregation filtering techniques. [5].

## 2. INTRODUCTION TO TRUST

The trust is the concept used in various contexts and with different meanings. Trust management is a useful technology to provide security service and its consequence has been used in many applications such as P2P, Grid, adhoc network and so on. Trust management (TM) plays very important role in IOT for reliable data fusion and mining, qualified services with context aware intelligence, and enhanced user privacy and information security. Trust is a complicated concept in terms of the confidence, reliability, integrity, security, and expectation on the dependability, ability, and other characters of an entity. This paper is focus on how to achieve trust level in IOT entities. IOT contains smart objects that are used to public areas and communicate through wireless network and vulnerable to arbitrary and malicious attacks. Smart objects have heterogeneous features and need to work together cooperatively.

lOT can provide the proper trust service according to his request, which will be translated to trust-related request.



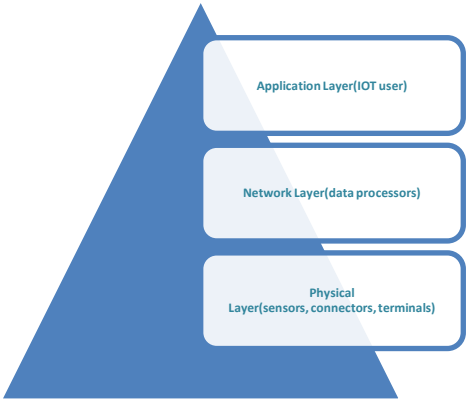
**Service Model**

### 2.1 Framework of Trust management for lOT

Network architecture of IOT system consists of three layers named as Physical layer/Sensor Layer , Network layer and Application layer.

Sensor layer contains series of physical devices and wireless sensor network. The main tasks of sensor network are collecting, perceiving information from physical world (physical environments and human social life). Network layer performs the operations to transforms and processes perceived environment data. It mainly provides inter-connecting and routing that transmits sensor information from the interface of gateway through access network and the internet to application layer. Application Layer provides context-aware intelligent services and interaction to end user in pervasive manner.

A trust worthy system is that which provides performance of whole of whole system in terms of security, privacy and other trust-related properties rather than to provide reliable data among layer. To ensure the trustworthiness of whole system trust can be achieved on every layer of IOT framework.




**2.2 Trust properties**

Trust is a measure of the quality of a relationship—between two people, between groups of people, or between a person and an organization Trust is a very complicated concept that is influenced by many measurable and non measurable properties. It is highly related to security purpose since ensures the system security and user safety is a necessary to gain trust. It relates not only security, but also many other factors, such as goodness, strength, reliability, availability, ability, or other characters of an entity. Although the richness of the concept, we can still summarize the subjective and objective properties that are relevant to a decision of trust. The properties influencing trust can be classified into five categories [6].

- Trustee ′s objective properties, such as a trustee ′s security (confidentiality, integrity, availability) and dependability. Particularly, reputation is a public assessment of the trustee regarding its earlier behavior,; strength, privacy preservation s and performance.
- Trustee ′s subjective properties, such as trustee honesty, benevolence, richness and goodness.
- Trustor ′s subjective properties, such as trustor belief, attitude, feeling, intention, faith, hope, disposition and willingness to trust.
- Trustor ′s objective properties, such as the criteria or policies, set of standards; trustor ′s standards specified by the trust or a trust decision.
- Context that the trust relationship resides in, such as the purpose of trust, the environment of and Situations entailing risk, structural, risk, domain of action, and the risk of trust. It specifies any information that can be used to characterize the background or situation of the involved entities [7].

**2.3 Objectives of trust management**

**Trust relationship and decision (TRD):** Trust management provides an effective way to evaluate trust relationships between IOT entities and make sure to take wise decision to communicate and collaborate with each other. Trust relationship evaluation (in short trust evaluation) concerns all IOT system entities in all layers and plays a fundamental role for intelligent and autonomic trust management.

**Data perception trust (DPT):** Data perception trust objective property of trust management in IOT should be achieved at physical perception layer. Data sensing and collection should be reliable in IOT. In this aspect, we mainly put attention to the trust properties like sensor sensibility, preciseness, integrity, confidentiality, security, reliability, and persistence, as well as data collection efficiency.

**Privacy preservation (PP):** This objective deals with user privacy including user data, user location and personal information should be flexibly preserved according to the policy and expectation of IOT users. This objective relates to the IOT system objective properties in general.

**Data fusion and mining trust (DFMT):**

The large amount of data collected in IOT should be processed and analyzed in a trustworthy way with regard to efficiency, security, reliability, holographic data process, privacy preservation and accuracy in the holistic manner. This objective also relates to trusted social computing in order to mine user demands based on their social behaviors and social relationship exploration and analysis. DFMT concerns the objective properties of the data processor in the IOT network layer.

**Data transmission and communication trust (DTCT)**

Trust should be assist while data is transmitted and communicated in the IOT system. Private data of others cannot be accessed by unauthorized system entities in data communications and transmission. This objective is related to the security and privacy properties of IOT system wherein light security/trust/privacy solution is needed [8].

## 3. LITERATURE SURVEY

**Xiaoyong Li , Feng Zhou, Xudong Yang in 2011** proposed **"A multidimensional trust evaluation model for largescale P2P computing"** that specifies innovative trust model for large scale peer-to-peer(P2P) computing, in which multiple factors are integrated to reflect the complexity of trust. This model overcomes the limitations of existing approaches, where weights are assigned subjectively and simulation results compared with the existing approaches, the proposed model provides greater accuracy and a more detailed analysis in trust evaluation [9].

**Yosra Ben Saieda, Alexis Olivereaua, Djamal Zeghlacheb, Maryline Laurentb in 2013** proposed "**Trust management system design for the Internet of Things: A context aware and multiservice approach"** that defines a new trust management system for internet of things which bound to assessment of trustworthiness with respect to single function. It overcomes the limitations of multifunction system which provides many restrictions to the adaptation of TMSs to today's emerging M2M and IOT architectures, which are characterized with heterogeneity in nodes, capabilities and services. This paper specifies trust objectives and trust properties and model how trust should be applicable on every layer of that model [10].

**S. Sicari , A. Rizzardi ,L.A. Grieco , A. Coen-Porisini in 2014** proposed **Security, privacy and trust in Internet of Things: The road ahead** specially defines main research challenges and the existing solutions in the field of IOT security, identifying open issues, and suggesting some hints for future research. This paper defines Suitable solutions that need to be designed and deployed, which are independent from the exploited platform and able to guarantee: confidentiality, access control, and privacy for users and things, trustworthiness among devices and users, compliance with defined security and privacy policies. [11].

**Shuaishuai Tan , Xiaoping Li , Qingkuan Dong in 2015** proposed **"Trust based routing mechanism for securing OSLR-based MANET"** which defines a trust reasoning model based on fuzzy Petri net is presented to evaluate

trust values of MANET which is wireless network that is self-organized by mobile nodes communicating with each other freely and dynamically to various fields such as emergency communications after disaster, intelligent transportation, and Internet of things. Trust based routing algorithm is proposed to select a path with the maximum path trust value among all possible paths. They extend OLSR by using the proposed trust model and trust based routing algorithm, called FPNT-OLSR [12].

**Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha in 2015** proposed **"Survey on secure communication protocols for the Internet of Things"** discusses the applicability and limitations of existing IP-based Internet security protocols and other security protocols used in wireless sensor networks, which are potentially suitable in the context of IOT.. In this paper they have discussed cryptographic operations i.e. based on RSA and Diffie–Hellman agreement protocols should be replaced by lightweight operations, i.e. using symmetric cryptography or applying more lightweight asymmetric cryptography and a trusted third party will also certainly take a more active role to secure the IOT and to adapt to its heterogeneous nature [13].

**Angelo Chianese, Francesco Picciallia, Giuseppe Ricciob in 2015** proposed **"The *TrUST* project: improving the fruition of historical centres through Smart Objects"** presents an on-going project named TrUST - Transport with Ubiquitous and Smart Technologies that aims to represent and manage the smartness inside transport coaches, adopting the IOT paradigm and supporting this direction with the design of a Smart Object. in this paper they Deploying a smart obects with GPS and WiFi capabilities, so that users can enjoy of multimedia content about the cultural heritage that surrounds them during a trip[14].

## 4. RESEARCH GAPS

The related work of trust management in IOT defines trust importance in IOT devices. Except for the above open issues in the literature, we are still facing a number of challenges related to trust management towards the final success of IOT in different application domains. Various applications and services of IOT have been emerging into markets in broad areas, e.g., surveillance, health care, security, transportation, food safety, and distant object monitor and control. The future of IOT is promising. For heterogeneous IOT, new demands for trust are in need. How to transmit and compute trust between different networks is a difficult problem.

## 5. CONCLUSIONS

When we look at today's state of the art technologies, we get a clear indication of how the IOT will be implemented on a universal level in the coming years. This report surveyed some of the most important aspects of IOT with particular focus on what is being done and what are the issues that require further research. While the current technologies make the concept of IOT feasible, a large number of challenges lie ahead for making the large-scale real-world deployment of IOT applications. We have studied here trust management will be a powerful driving force for networking and communication research in both industrial and academic laboratories. There is still need to implement IOT challenges trust management in different fields of IOT. I will implement trust management in Transportation using IOT devices.

**REFERENCES**

[1]http://whatis.techtarget.com/definition/Internet-of-Things

[2]www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf

[3]www.academia.edu/3276195/Internet_of_Things_Applications_and_Challenges_in_Technology_and_Standardization

[4] J.Gubbi, "Internet of things (IOT): A viosion", *Future Generation Computer Systems*, pp, 1645-1646,2013.

[5]www.academia.edu/3276195/Internet_of_Things_Applications_and_Challenges_in_Technology_and_Standardization

[6] Yan and Holtmanns, 2008 and Yan and Prehofer, 2011

[7] Dey, 2001

[8]Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," J. Netw. Comput. Appl., vol. 42, pp. 120–134, 2014.

[9] Xiaoyong Li , Feng Zhou, Xudong Yang in 2011

[10] Yosra Ben Saieda, Alexis Olivereaua, Djamal Zeghlacheb, Maryline Laurentb in 2013

[11] S. Sicari , A. Rizzardi ,L.A. Grieco , A. Coen-Porisini in 2014

[12] Shuaishuai Tan , Xiaoping Li , Qingkuan Dong in 2015

[13] Kim Thuat Nguyen , Maryline Laurent, Nouha Oualha in 2015

[14] Angelo Chianese, Francesco Picciallia, Giuseppe Ricciob in 2015