IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 23-26

Review of Recent Trends in Internet of Things

Prof. N.A. Rathod[1], Prof. P.H. Jadhao[2], Dr. A. B. Raut[3]
[1]*Department of CSE H.V.P.M COET,Amravati*
[2]*Department of CSE G.H.Raisoni,Amravati*
[3] *HOD,Department of CSE H.V.P.M COET,Amravati*

Abstract: *The Internet of Things (IOT) is the vast immerging technology in the field of communication networks. It is estimated that billions of devices will be connected to internet in near future. This paper provides the introduction to concept of Internet of things and recent trends in IOT. Managing transient data of sensor connected to IOT devices is issue of concern. IOT system analyzes the indoor environmental condition many predictive model are developed. Security of IOT system and application is also key area of concern, secure communication and firewall protection can help IOT system from different security attacks. Paper review all above mention areas and try to present basic of IOT and recent work in field of Internet of Things.*

I. Introduction

The world has seen emergence of World Wide Web in decade of 90's later on number of devices connected to internet went on increasing exponentially. IOT emerged as phenomenon where different objects are connected to internet. The term Internet of things refers to that Machine-to-Machine communication happens between two things over internet. The core concept of IOT is that objects in day to day life are equipped with indentifying, sensing, networking and processing capabilities which enables them to communicate and give services over the internet for achieving objectives. IOT enables the objects see, think, communicate and perform task by communicating together and make decision. IOT transform these ordinary objects to smart by making use of technologies like embedded devices, communication technologies, sensor networks, Internet protocols and applications. In near future, the IOT is expected to have significant home and business applications, to contribute to the quality of human life and to grow the world's economy. There are also other domains and Environments in which the IOT can play a remarkable role and improve the quality of our lives. These applications include transportation, healthcare, industrial automation, and emergency response to natural and man-made disasters where human decision making is difficult.

It is estimated that by 2020 over 50 billion devices will be connected to the Internet. This much amount of data results in a classic Big Data problem, the need to extract process and analyze this data. The sensors which gather data over internet produce transient data. The transient data is non persistent data whose usefulness decreases rapidly with the time. Managing this huge amount transient data is problem and need to be addressed. Vast industrialization and mankind's ignorance towards nature has caused pollution of environment which is biggest area of concern for human beings survival on planet. Internet of Things has both positive and negative impacts on the environment. IOT can help in controlling air pollution which is one of the leading challenges in environmental hazards. The urban area is more affected with air pollution especially with indoor pollution. As people spend more time in home, office or any other indoor place indoor pollutant like CO, CO_2, and VOC can cause hazardous heath problems. The indoor air quality control is important to avoids health issues. Our goal is to design a low cost, high precision, portable device capable of measuring the concentration of most of the indoor environmental pollutants.

Most important issue is security of IOT devices from different type of security attacks which can breach confidentiality, integrity, and authentication and eventually break down system. Security services, architectures and firewalls gives good defense to different attacks. This paper proceeds as follows: section II describe Managing Transient data in IOT followed by Indoor environment prediction in section III. Section IV describes security in IOT, paper concludes by section V conclusion.

II. Managing Transient Data In Iot

In above section generation of transient data at sensors in IOT system is discussed. The managing enormous amount of transient data is important which poses some of the important challenges as follows:

a) Defining which data is transient.
b) Designing IOT network to handle volume of data.
c) How to place transient data in IOT network so that latency of data transmission minimize.

d) How to determine that subset of data in data server that needs to be sent to a central cloud server for storage.
e) How to use provenance to determine which data to be sent to the central cloud server? Provenance, i.e., history of past usage, can, in addition to the actual nature of the data itself, dictate which data needs to be stored in the central cloud server.
f) How to use history of past usage of data to determine which data to be sent to the central cloud server.

Following are components of proposed system for managing transient data [3]:

Characterization of Transient data is responsible for minimizing data sets as transient data and their associated storage. Resource Estimator is required for estimate transient data sets involved in data pipeline also compute processing requirement. Resource planner matches storage and calculate resources requirement with different location.

Data Manager performs actions of minimizing

Association between data sets, tracking data and deriving possible optimizations such as temporary data migration or transformation for a data set. System maintain registry of storage for computing it on edge, fog and cloud. User can use Domain specific language for data processing. Characterization of transient data involves identifying its characteristics like generation source(s), validity period, estimated storage volume, etc. After characterization of transient data is done system performs the matching of available storage and estimated capabilities of transient data sets. The system formulates the data flow as a Direct Acyclic Graph (DAG) model consist of computation and storage units, based on the identified data processing elements and data sets involved. And then the system deploys the DAG units as per the model.

The transient data is categorized from the data of sensor it is identified and marked then it is processed with help of provenance based intelligent data management model. At last domain specific language rule and policies of implemented system will deduce computation requirements for a data flow described in such a goal, and match them with available capabilities while attempting to optimize costs.

III. Indoor Environment

PREDICTION BY IOT

The people in urban cities are affected with indoor pollution. Gases like COE, CO, VOC can cause serious problem with heath of people. Following are three different research problem identified in [4].

a) Developing intelligent environment monitoring devices using low cost sensor: proposed solution consist of environment monitoring devices consist of 3 modules. Power module, microcontroller and sensing module. These devices are able to measure concentration of CO, CO2, and NO2 particulate matter humidity using Bluetooth and Wi-Fi module as communicating devices.
b) Calibration of sensor machine learning using machine learning techniques: To achieve the error free system, different types of machine learning techniques can be used. Sensors have to be calibrated using internal calibration n. Data sets collected from different sensor has to analyzed and verified through environment monitoring box(EMB). Regressions have to applied on collected data set from the sensors and formulate the error as a faulty data. Next step will be to formulate a generalized model such that it can work in any condition despite Spatio-temporal changes.
c) Design of IOT-enabled ventilators system by prediction of pollutants in indoor environment :
IOT based ventilators are necessary in for rooms which suffers the concentration of indoor pollution after one or two hour of continuity. To reduce cost of energy utilization, triggering of IOT system should happen according to the need. The level at which class room indoor pollution cross a threshold (acceptable level of pollution) triggering of event should happen. Starting of ventilating system before class room start would be good solution of prohibiting the indoor pollution of room.

IV. Security In Iot

The attacker or intruders can exploit vulnerabilities in IOT system like programming errors, web based vulnerability, weak access control, authentication and inappropriate use of cryptography. They may launch different attacks on IOT system which may breach authentication, confidentiality, and integrity. There is need of providing security mechanism to IOT system. In IOT security architecture [5] decentralization and authorization is proposed by using local certification Authority (CA).

a) Local CA:

In a Public key Encryption (PKI) Certification Authority (CA) is a third party that provides certificates to servers. The two entities must have certificate signed by CA so that they can communicate with each other.

We can use public-private asymmetric key pair to certify/verify public modules of all the entities. Henceforth, this public private asymmetric key pair is referred to as local CA.

b) Auth:

Auth controls the communication between all entities in the network. Being an entity, Auth also needs to have a certificate signed by the local CA. To provide service of communication between entities, Auth has to maintain four tables as given below:

- Group Table: Contains information about the validity period for a given group name.
- Entity Table: Contains information of all the registered entities, which includes Entity Name, Group Name, and Public Key, Distribution key, validity, IP address and Destination Port address.
- Access Table: Contains information regarding authorization of an entity.
- Session Table: Contains information regarding active sessions between all the entities in network, such as session keys and their validities. Information is erased if validity of the session is over.

c) Stages of secure communication:

For secure communication to happen it need to go through three stages registration, session key distribution and communication. In registration stage Auth verify identity and information of different entities and register them, now these entities become part of network their communication Auth and entity is secure using Distribution keys.

In session key distribution stage two entities which are client and server. Here client entity request Auth to grant communication session with server entity ,if allowed Auth grant secure communication between two entities by distributing session key. In last stage which is communication happen between client entity and server entity using session key.

V. Conclusion

In this survey paper, we have discussed recent trends in field of Internet of Thing. The main area of survey was transient data management in IOT system, controlling Indoor Environment of Rooms pollution with help of IOT application and system last was security of IOT application and system from different highly sophisticated attacks. The paper discuss challenges and proposed solution found in survey of different paper in transient data management, also paper discuss specifically about air pollution in indoor rooms and discuss probable solution of survey. The security of the IOT system is emerging field the proposed solution of security of IOT system is discussed.

References

[1]. Alem Colakovic, Mesud Hadzialic "Internet of Things (IOT): A Review of Enabling Technologies, Challenges, and Open Research Issues" Elsevier journal Computer Network, Vol. 144,17-39

[2]. Mehdi Mohammadi, mohammad Aledhari "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications" IEEE Communication Survey & AMP Tutorials, Jan 2015.

[3]. Nanjangud C. Narendra, Sambit Nayak, Anshu Shukla "Managing Large-Scale Transient Data in IoT Systems" 10th International conference on communication System & Networks, 3-7 Jan 2018

[4]. Praveen Kumar Sharma, Tanmay De, Sujoy Saha "IoT based indoor environment data modelling and prediction" 10th International conference on communication System & Networks, 3-7 Jan 2018

[5]. Navinkumar Maheshwari , Haresh Dagale "Secure Communication and Firewall Architecture for IoT Applications**"** 10th International conference on communication System & Networks, 3-7 Jan 2018

[6]. Prathibha S R, Anupama Hongal , Jyothi M P **"**IOT based monitoring system in Smart agriculture**"** International Conference on Recent Advances in Electronics and Communication Technology 2017

[7]. Suraj Choudhari, Tejas Rasal, Shubham Suryawanshi, Mayur Mane, Prof. Satish Yedge "Survey Paper on Internet of Things: IoT" IJESC Vol. 7 Issue No. 4

[8]. C. Cecchinel, M. Jimenez, S. Mosser, and M. Riveill, "An architecture to support the collection of big data in the internet of things," pp. 442–449, 2014.

[9]. M. Fazio, A. Puliafito, and M. Villari, "Iot4s: a new architecture to exploit sensing capabilities in smart cities," *International Journal of Web and Grid Services*, vol. 10, no. 2, pp. 114–138, 2014.

[10]. F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 2012, pp. 13–16.

[11]. D. Preuveneers and Y. Berbers, "Samurai: A streaming multi-tenant context-management architecture for intelligent and scalable internet of things applications," pp. 226–233, June 2014.

[12]. M. Antunes, D. Gomes, and R. Aguiar, "Scalable semantic aware context storage," pp. 152–158, Aug 2014.

[13]. Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan "Towards an analysis of security issues, challenges, and open problems in the internet of things" *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015.

[14]. Gupta, M. Surya Deekshith et al. "Healthcare based on IoT using Raspberry Pi." *Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on*. IEEE, 2015.

[15]. Zhang, Yuanyu, et al. "On secure wireless communications for IoT under eavesdropper collusion." *IEEE Transactions on Automation Science and Engineering 13.3* (2016): 1281-1293.

[16]. Wrona, Konrad. "Securing the Internet of Things a military perspective." *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 2015.
[17]. Yang, Yuchen, et al. "A Survey on Security and Privacy Issues in Internetof- Things." *IEEE Internet of Things Journal (2017)*.
[18]. Kim, Hokeun, et al. "A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities." *Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on*. IEEE,2016.
[19]. A. Ghosh, S. Mondal, M. Saha, S. Saha, and S. Nandi, "Poster: Air quality monitoring using low-cost sensing devices," in *MobiSys 2016*, pp. 27–27.
[20]. K. B. Shaban, A. Kadri, and E. Rezk, "Urban air pollution monitoring system with forecasting models," *IEEE Sensors Journal*, vol. 16, no. 8,pp. 2598–2606, 2016