ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 38-44

Data Aggregation, Security Control and Device Addressing Over WSN in IoT

Manas Ranjan Moharana[1] , Bikash Chandra Pattanaik[2]

[1]*(Computer Science & Engineering, Gandhi Institute For Education & Technology Bhubaneswar, India)*
[2]*(Computer Science & Engineering, Gandhi Institute For Education & Technology Bhubaneswar, India)*

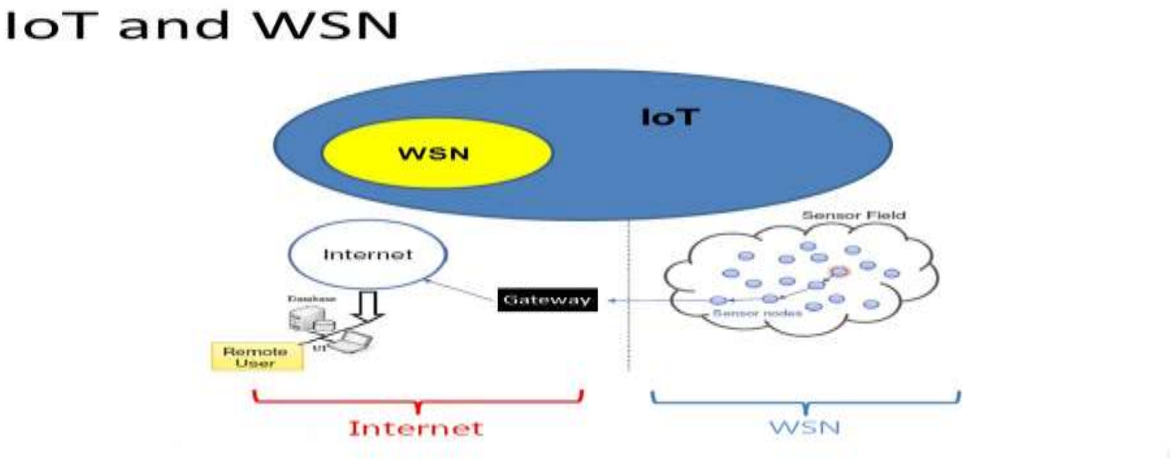
Abstract: *A sensor interface device is important for sensor data collection of industrial wireless sensor networks (WSN) in IoT environments. However, the current connect Number, sampling rate, and types of sensors are restricted by the device. Meanwhile, in the Internet of Things (IoT) environment; each sensor connected to the device is required to write complicated and cumber some data collection program code. In IoT environment base of sensor are used improper use of power including non-standard addressing scheme and lack of device security In this paper, to solve these problems, we proposed are IoT based network to overcome all problems to developed IoT based network using integration of hash based addressing scheme for device by developing data aggregation to reduce power consumption and also provide Kerberos based authentication system for device control so that our IoT based environment will be used for all environment monitoring security. Design a reconfigurable smart sensor interface for industrial WSN in IoT environment, in which complex programmable logic device (CPLD) is works as the core controller. Thus, it can read data in parallel and in real time system with high speed on multiple different sensor data. The standard of IEEE1451.2 intelligent sensor interface specification is adopted for this design. It combine stipulates the smart sensor hardware and software design framework and relevant interface protocol to realize the intelligent acquisition for common sensors .A new solution is provided for the general sensor data acquisitions. The device is combined with the newest CPLD programmable technology and the standard of IEEE1451.2 intelligent sensor specification. Performance of the proposed system is verified and good effects are achieved in practical application of IoT.*

Keywords *– Internet of Things, Cloud Computing, Wireless Sensor Network, CPLD.*

I. Introduction

Smart connectivity with existing networks and context-aware computation by using network resources is necessary part of IoT. With the growing presence of Wi-Fi and 4G-LTE wireless Internet access, the evolution towards existing information and communication networks is already evident. However, for the Internet of Things vision to successfully emerge, the computing paradigm will need to go beyond mobile computing scenarios that use smart phones and portables, and evolve into connecting everyday existing objects and embedding intelligence into our environment. For technology to disappear from the consciousness of the user, the Internet of Things demands: (1) a shared understanding the situation of users and their appliances, (2) software architectures and penetrating communication networks to process and convey the information to where it is relevant, and (3) the analytics tools in the Internet of Things that aim for autonomous and smart behavior. With these fundamental grounds in place, smart connectivity and context-aware computation can be accomplished.

Wireless sensor network (WSN) is a group of spatially interspersed and working the sensors for monitoring and recording the physical conditions of the environment and maintaining the collected data at the central sensor node. Generally, WSN measures the environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, speed etc. A fig1 consist the number of nodes which are able to interact with environment by sensing and controlling the physical parameters. Initially wireless sensor network used by only military field for various operations but nowadays used in various field like health, traffic and many other industrial areas. Cloud computing technologies have been intensively exploited in development and management of the large-scale IoT systems, because theoretically, cloud offers unlimited storage, compute and network capabilities to integrate diverse types of IoT devices and provide an elastic runtime infrastructure for IoT systems. Self-service, utility oriented model of cloud computing can potentially offer fine grained IoT resources in a pay-as-you-go manner, reducing front end costs and possibly creating cross-domain application opportunities and enabling new business and usage models of the IoT cloud systems.



II. Objectives

- Development of an IoT based network.
- Integration of a hash based addressing scheme for devices.
- Development of data aggregation to reduce power consumption.
- Provide Kerberos based authentication for device control.

Wireless Sensor Network (WSN) technologies cuts across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet.

The evolution of the next generation mobile system will depend on the creativity of the users in designing new applications. IoT is an ideal emerging technology to influence this domain by providing new evolving data and the required computational resources for creating revolutionary apps. Presented here is a user-centric cloud based model for approaching this goal through the interaction of private and public clouds. In this manner, the needs of the end-user are brought to the fore. Allowing for the necessary flexibility to meet the diverse and sometimes competing needs of different sectors, we propose a framework enabled by a scalable cloud to provide the capacity to utilize the IoT.

The framework allows networking, computation, and storage and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment. The standardization which is underway in each of these themes will not be adversely affected with Cloud at its center. In proposing the new framework associated challenges have been highlighted ranging from appropriate interpretation and visualization of the vast amounts of data, through to the privacy, security and data management issues that must underpin such a platform in order for it to be genuinely viable. The consolidation of international initiatives is quite clearly accelerating progress towards an IoT, providing an overarching view for the integration and functional elements that can deliver an operational IoT.

Internet of Things (IoT): It is estimated there are over a billion internet users and rapidly increasing. But there are more things on the internet than there are people on the internet. This is what we generally mean when we say internet of things. There are millions and millions of devices with sensors that are linked up together using networks that generate a sea of data. With the benefit of integrated information processing capacity, industrial products will take on smart capabilities. They may also take on electronic identities that can be queried remotely, or be equipped with sensors for detecting physical changes around them. Such developments will make the merely static objects of today dynamic ones - embedding intelligence in our environment and stimulating the creation of innovative products and new business opportunities. The Internet of Things will enable forms of collaboration and communication between people and things, and between things themselves, so far unknown and unimagined. With continuing developments in miniaturization and declining costs, it is becoming not only technologically possible but also economically feasible to make everyday objects smarter, and to connect the world of people with the world of things. Building this new environment however, will pose a number of challenges. Technological standardization in most areas is still in its infancy, or remains fragmented. Not surprisingly, managing and fostering rapid technological innovation will be a challenge for governments and industry alike. But perhaps one of the most important challenges is convincing users to adopt emerging technologies like RFID. Concerns over privacy and data protection are widespread, particularly as sensors and smart tags can track a user's movements, habits and preferences on a perpetual basis. Fears related to nanotechnology range from bio-medical hazards to robotic control. But whatever the concern, one thing remains clear: scientific and technological advances in these fields continue to move ahead at breakneck speed. It is only through awareness of such advances, and the challenges they present, that we can reap the future benefits of a fair, user-centric and global Internet of Things.

This project is about allowing users to get information, knowledge and wisdom from sensor data by using the power of cloud computing and to achieve that in a scalable and economical way. We develop a web application to be made available as a software as a service (SaaS) for sensor data analytics and visualization. It was essentially a proof of concept application to show that it is possible to analyze and visualize large sensor datasets efficiently and economically using the power of cloud computing.

Cloud computing is ever stronger converging with the Internet of Things (IoT) offering novel techniques for IoT infrastructure virtualization and its management on the cloud. However, system designers and operations managers face numerous challenges to realize IoT cloud systems in practice, mainly due to the complexity involved with provisioning large-scale IoT cloud systems and diversity of their requirements in terms of IoT resources consumption, customization of IoT capabilities and runtime governance. In this paper, we introduce the concept of software-defined IoT units – a novel approach to IoT cloud computing that encapsulates fine-grained IoT resources and IoT capabilities in well-defined APIs in order to provide a unified view on accessing, configuring and operating IoT cloud systems. Our software-defined IoT units are the fundamental building blocks of software-defined IoT cloud systems.

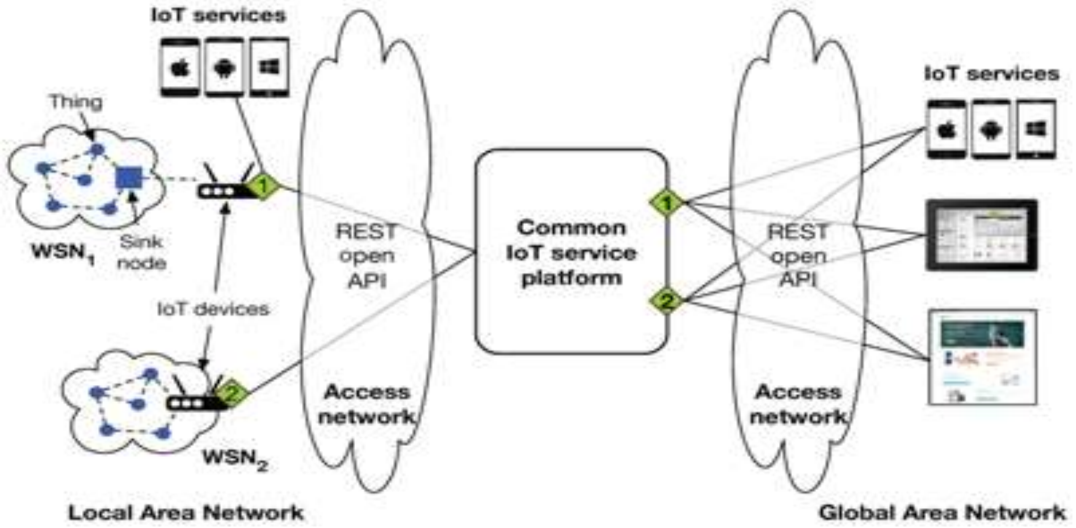
We demonstrate its advantages on a real-world IoT cloud system for managing electric fleet vehicles. They introduced the conceptual model of software-defined IoT units. To our best knowledge this is the first attempt to apply software-defined principles on IoT systems. We showed how they are used to abstract IoT resources and capabilities in the cloud, by encapsulating them in software-defined API. We presented automated unit composition and managed configuration, the main techniques for provisioning software-defined IoT systems. The initial results are promising in the sense that software-defined IoT system enables sharing of the common IoT infrastructure among multiple stakeholders and offer advantages to IoT cloud system designers and operations managers in terms of simplified, on demand provisioning and flexible customization. Therefore, we believe that software-defined IoT systems can significantly contribute the evolution of the IoT cloud systems.

III. Problem Statement

IoT is the future of technology which will decide how we control and interact with our day to day devices and make them more efficiently. The scheme main problem with IoT is improper use of power, non standers addressing scheme and lack of device security. Our problem statement is to remove all the three drawbacks.

IV. Implementation

1. The addressing of device will be done based on a secure hashing algorithm. (SHA) where each device ID will be first hash and then used for device tracking and control.
2. For data aggregation we will be using a threshold based aggregation scheme this will reduce total number of byte communicated there by reducing the power consumption.
3. The Kerberos based security system will be developed for authentication of user.
4. The overall system architecture can be describe as fallows.



Wireless sensor networks (WSN) are recognized key enablers for the Internet of Things (IoT) paradigm since its inception. WSNs are a resilient and effective distributed data collection technology, but issues related to reliability, autonomy, cost, and accessibility to application domain experts still limit their wide scale use. Commercial solutions can effectively address vertical application domains, but they often lead to technology lock-ins that limit horizontal compos ability and reuse. We review some important barriers that hinder WSN use in IoT applications and highlight the main effort and cost components. With these elements in mind, we propose an open hardware-software development platform that can optimize the value flow between technologies and actors with stakes in WSN applications. recent technological advances in low power integrated circuits and wireless communications have made available efficient, low an appropriate topology, routing and MAC layer is critical for the scalability and longevity of the deployed network. Nodes in a WSN need to communicate among themselves to transmit data in single or multi-hop to a base station. Node drop outs, and consequent degraded network lifetimes, are frequent. The communication stack at the sink node should be able to interact with the outside world through the Internet to act as a gateway to the WSN subnet and the Internet.

WSN Middleware: A mechanism to combine cyber infrastructure with a Service Oriented Architecture (SOA) and sensor networks to provide access to heterogeneous sensor resources in a deployment independent manner [17]. This is based on the idea of isolating resources that can be used by several applications. A platform-independent middleware for developing sensor applications is required, such as an Open Sensor Web Architecture (OSWA) [18]. OSWA is built upon a uniform set of operations and standard data representations as defined in the Sensor Web Enablement Method (SWE) by the Open Geospatial Consortium (OGC).

Secure Data aggregation: An efficient and secure data aggregation method is required for extending the lifetime of the network as well as ensuring reliable data collected from sensors Node failures are a common characteristic of WSNs, the network topology should have the capability to heal itself. Ensuring security is critical as the system is automatically linked to actuators and protecting the systems from intruders becomes very important.

To avoid the above mentioned problems, data aggregation techniques have been introduced. Data aggregation is the process of integrating multiple copies of information into one copy, which is effective and able to meet user needs in middle sensor nodes. Data aggregation technology could save energy and improve information accuracy, while sacrificing performance in other areas. On one hand, in the data transfer process, looking for aggregating nodes, data aggregation operations and waiting for the arrival of other data are likely to increase in the average latency of the network. On the other hand, compared to conventional networks, sensor networks have higher data loss rates. Data aggregation could significantly reduce data redundancy but lose more information inadvertently, which reduces the robustness of the sensor network.

Addressing schemes: The ability to uniquely identify ‘Things’ is critical for the success of IoT. This will not only allow us to uniquely identify billions of devices but also to control remote devices through the Internet. The few most critical features of creating a unique address are: uniqueness, reliability, persistence and scalability. Every element that is already connected and those that are going to be connected, must be identified by their unique identification, location and functionalities. The current IPv4 may support to an extent where a group of cohabiting sensor devices can be identified geographically, but not individually. The Internet Mobility attributes in the IPV6 may alleviate some of the device identification problems; however, the heterogeneous nature of wireless nodes, variable data types, concurrent operations and confluence of data from devices exacerbates the problem further . Persistent network functioning to channel the data traffic ruinously and relentlessly is another aspect of IoT. Although, the TCP/IP takes care of this mechanism by routing in a more reliable and efficient way, from source to destination, the IoT faces a bottleneck at the interface between the gateway and wireless sensor devices. Furthermore, the scalability of the device address of the existing network must be sustainable. The addition of networks and devices must not hamper the performance of the network, the functioning of the devices, the reliability of the data over the network or the effective use of the devices from the user interface. To address these issues, the Uniform Resource Name (URN) system is considered fundamental for the development of IoT. URN creates replicas of the resources that can be accessed through the URL. With large amounts of spatial data being gathered, it is often quite important to take advantage of the benefits of metadata for transferring the information from a database to the user via the Internet. IPv6 also gives a very good option to access the resources uniquely and remotely. Another critical development in addressing is the development of a lightweight IPv6 that will enable addressing home appliances uniquely.

Data storage and analytics: One of the most important outcomes of this emerging field is the creation of an unprecedented amount of data. Storage, ownership and expiry of the data become critical issues. The internet consumes up to 5% of the total energy generated today and with these types of demands, it is sure to go up even further. Hence, data centers that run on harvested energy and are centralized will ensure energy efficiency as well as reliability. The data have to be stored and used intelligently for smart monitoring and actuation. It is important to develop artificial intelligence algorithms which could be centralized or distributed based on the need. Novel fusion algorithms need to be developed to make sense of the data collected. State-of-the-art non-linear, temporal machine learning methods based on evolutionary algorithms, genetic algorithms, neural networks, and other artificial intelligence techniques are necessary to achieve automated decision making.

Sensor Network Security: Sensor network technology in IoT exploit a number of sensor nodes, thus allowing the acquiring, processing, analysis and distribution of vital information, gathered across the network. Resource restriction in some applications of sensor networks causes them to work without security thus decreasing the Quality of Service (QoS) [36]. The major security attacks on sensor networks and cryptographic method to deal with those attacks are discussed in this section. 1) Sensor Network Attacks The sensor networks are susceptible to a number of attacks. These attacks can be categorized according to the security requirements as follows [37]: Secrecy and authentication: the outsider attacks on• secrecy and authentication of sensor networks, such as eavesdropping, replay attacks, modification of packets, or spoofing can be minimized by using cryptographic techniques. Network availability: the attacks on availability of• network are commonly referred to as Denial of Service (DoS) attacks. Sensor networks are divided into layers making them more susceptible to DoS attacks, as these attacks can occur in any layer of sensor networks. Service integrity: the goal of attacker in these attacks is• to make the network accept wrong data values.

Attacks Based on Layering The protocol stack of sensor networks is composed of five layers viz. physical layer, data link layer, network layer, transport layer, and application layer authentication, and by monitoring the network against harmful nodes .

Secure data aggregation of WSNs: Secure data aggregation is to ensure each node data is secure. Therefore, the general processes of secure data aggregation are as follows: first nodes should be possible to provide reliable date and securely transmit them to the higher aggregation nodes. The higher aggregation nodes judge the credibility of data and do aggregation calculation based on redundancy. Each aggregation nodes select the next safe and reliable hop, transmit data to the central node. The central nodes judge the credibility of data and do the final aggregation calculation. Initially, data aggregation regarded energy as the object and barely considered security issues. Now secure data aggregation is mostly realized by authentication and encryption based on the theory of cluster, ring, and hierarchical. The University of Munich developed a data aggregation prototype, which is based on DTLS protocol to realize secure transmission schemes. The red circle of Figure 3-16 represents their secure data aggregation prototype.

V. Benefits of WSN

Improve energy efficiency

As an effective means to acquire information, it can implement real-time monitoring over the operation of energy conversion, and make timely analysis and processing of the large amount of data. In addition, it can also make speedy responses to abnormal status and guarantee the system security as it can enable a valid management of the whole process (from generation to transportation and usage) of the energy system in fi ne grain and dynamic mode.

Contribute to environmental monitoring

Environment pollution, sudden natural and ecological disasters and man-made damages are still the major environmental problems that need to be resolved at present. Early detection, alarming and initiation of emergency measures are key steps to avoid great environment disasters. IoT, featuring a powerful sensing ability and wide coverage of detecting area, can make a real-time and all around monitoring over the environment. In this sense, with a data fusion and intelligent recognition technology, it can increase the alarming efficiency.

Enhance social services

IoT offers a way for different elements in social services to relate and connect with each other through the internet: man, equipment, and social service resources. Thanks to IoT, on one hand, the service providers can obtain information about people's demands and provide them tailored and high-quality services; while on the other hand, people can have a better understanding of themselves and the environment around them. It is safe to predict that IoT will change people's lifestyles in some aspects. For example, IoT-based smart health care and smart home systems will bring more convenience and comfort to people's lives.

VI. To improve IoT Device security

Secure and centralize the access logs of IoT devices: Preventing devices from connecting to the network without IT's knowledge is one of the first lines of defense. IT managers maintain centralized access logs of networks under their control. They know what's attached to the network and who logs in to what, when, and for how long. Unfortunately, the process hasn't scaled to address the volume of IoT devices coming online, which has enabled hackers to enslave insecure devices into bonnets to launch distributed denial-of-service (DDoS) attacks. The consequences can be considerable. Thousands of vulnerable routers, IP cameras, and digital video recorders became infected with the Mirai malware and were then used to take down major websites. Mirai spreads to vulnerable devices by continuously scanning the Internet for IoT systems that are protected by factory default or hard-coded usernames and passwords.

Use encrypted protocols to secure communications: Encryption practices of IoT devices are inferior and insecure. Few devices use encrypted communications as part of their initial configuration. Rather, most use ordinary web protocols that communicate across the Internet in plain text, which makes them easy targets for hackers observing network traffic to identify weaknesses. At the very least, all web traffic should be using HTTPS, transport layer security (TLS), Secure File Transfer Protocol (SFTP), DNS security extensions, and other secure protocols for communications with management stations and across the Internet. In addition, devices that connect to mobile apps or other remote gateways should use encrypted protocols as well as encrypt data stored on flash drives. One reason to encrypt data is to ensure that malware hasn't infected the device.

Implement restrictive network communications policies, and set up virtual LANs: It's important to understand the difference between restrictive network communications and permissive network communications. For example, there is a difference between a PC that shares all of its hard drive with everyone and a web server that restricts only a few authorized users to view its content. Unlike most restricted web servers, the assumption with IoT devices—such as temperature sensors—is that they are permissive. They can and should communicate with just about anyone and any device by default. This permissive communication is part of their design. Vendors want them to participate on networks and share their data with a variety of tools and software programs. Unfortunately, permissiveness is what makes these devices inherently insecure and vulnerable to all sorts of exploits. Instead, restrictive network communications, such as built-in firewall rules or more careful user or application authentication, should be implemented. Devices should not be reachable by standard TCP/IP ports users should not assume they operate behind enterprise firewalls that will prevent communications across such as Telnet or FTP, and the network or out to the Internet.

Design explicitly for privacy and security:

Few IoT device vendors consider security a feature or incorporate it into the design lifecycle. As a result, most devices fail to offer privacy policies or incorporate privacy-by-design principles. (This is also true of many standard computer hardware and software vendors.) In addition, distinguishing between the roles of supplier, OEM, customer, and partner is getting harder, making enforcement of security best practices difficult. As a result, some devices might have inserted malware, outdated software, bugs, or other vulnerabilities due to lack of proper testing or quality controls.

Improve failover design: Devices should function when Internet connectivity is lost or disrupted. However, few IoT devices are designed to cope with failures such as Internet continuity or data disconnections. Failover design is especially important for IoT devices that involve user safety, such as door lock mechanisms, video monitoring, and environmental monitors and alarms. These devices should have manual overrides or special functions for disconnected operations.

Acknowledgment

This paper is aimed towards implementation of WSN for environment monitoring in IoT by suggesting solutions for various problems faced while implementing WSN in real world. All requirements of IoT to be achieved from WSN and functional specifications are studied here.

VII. Conclusion

Internet of things is an emerging field which has improved the quality of human life with its vast automated applications. The functionalities provided by IoT can save time and computational power of users to help improve results in the diverse application areas. This paper presented the overview of the enabling technologies and applications of IoT in different fields. Further, some of the security issues regarding the wireless technologies involved in deployment of IoT are presented along with their possible countermeasures. The future of internet is IoT, but there is still a need for further research in this field because of the ever increasing demands of users.

An efficient system for parameter monitoring and device control has been built, and tested with real time sensors and actuators IoT is the future of technology which will decide how we control and interact with our day to day devices and make them more efficiently.

We can add the concept of machine learning and artificial intelligence in the system in order to get more efficient data collection and control. Presented here is a user-centric cloud based model for approaching this goal through the interaction of private and public clouds. In this manner, the needs of the end-user are brought to the fore. Allowing for the necessary flexibility to meet the diverse and sometimes competing needs of different sectors, we propose a framework enabled by a scalable cloud to provide the capacity to utilize the IoT. The framework allows networking, computation, storage and visualization themes separate thereby allowing independent growth in every sector but complementing each other in a shared environment. The standardization which is underway in each of these themes will not be adversely affected with Cloud at its center. In proposing the new framework associated challenges have been highlighted ranging from appropriate interpretation and visualization of the vast amounts of data, through to the privacy, security and data management issues that must underpin such a platform in order for it to be genuinely viable.

References

[1]. Rogers, Moving on from Weiser′s vision of calm computing: engaging ubicomp experiences, in: UbiComp 2006: Ubiquitous Computing, 2006.

[2]. R. Caceres, A. Friday, Ubicomp systems at 20: progress, opportunities, and challenges, IEEE Pervasive Computing

[3]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks

[4]. L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805.

[5]. J. Belissent, Getting clever about smart cities: new opportunities require new business models, Forrester Research, http://www.gartner.com/technology/research/hype-cycles/.

[6]. Google Trends, Google (n.d.). http://www.google.com/trends.

[7]. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing .

[8]. S. Tilak, N. Abu-Ghazaleh, W. Heinzelman, A taxonomy of wireless microsensor network models, ACM Mobile Computing and Communications .

[9]. Jayavardhana gubbi, Rajkumar buyyab,, Slavenmarusic, Marimuthu palaniswami "Internet Of Things (Iot): A Vision, Architectural Elements, And Future Directions" Future Generation Computer Systems.

[10]. Kumar swamy Krishna kumar "Data Analytics and Visualization in Cloud Computing Environments" Distributed Computing Project COMP90019, University Of Melbourne,

[11]. Stefan Nastic, Sanjinsehic, Duc-Hung Le, Hong-Linh Truong, And Schahramdustdar" Provisioning Software-Defined Iot Cloud Systems "Distributed Systems Group, Vienna University Of Technology, Austria

[12]. Jitendra Pal Thethi "Realizing the Value Proposition of Cloud Computing" CIO's Enterprise IT Strategy for Cloud.