# DESIGN AND DEVELOPMENT OF COMMUNICATION NETWORKS USING IOT

**M. Jayaprakash[1], V. Kumara Swamy[2], V. Senthil[3], Suresh Kumar Maddila[4],**

**M Anusuya[5], Sumit Kushwaha[6]∗**

[1]Department of Information Technology, R. M. K Engineering College, Kavaraipettai, Tamil Nadu 601206, India. **mjh.it@rmkec.ac.in**

[2]Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana 501301, India. **ksvarkuti@gmail.com**

[3]Department of Electronics and Communication Engineering, JKK Nattraja College of Engineering and Technology, Komarapalayam, Tamil Nadu 638183, India. **senthil.vlsi84@gmail.com**

[4]Department of Computer Science, GITAM School of Science, Gandhi Institute of Technology and Management, Visakhapatnam, Andhra Pradesh 530045, India. **smaddila@gitam.edu**

[5]Department of Physics, Indra Ganesan College of Engineering, Trichy, Tamil Nadu 620012, India. **sarananu94@gmail.com**

[6]Department of Computer Applications, University Institute of Computing, Chandigarh University, Gharuan, Punjab 140413, India. **sumit.kushwaha1@gmail.com**

*Corresponding Author*: **sumit.kushwaha1@gmail.com**

Abstract:-

The development of software engineering applications that provide automated solutions has made it possible to create tools and gadgets that ease everyday tasks. Technology is presently an important benchmark in all application areas. In this sense, this work suggests two architectures that make use of the GSM/GPRS communication services as well as the Twitter social network to enable remote communication between the electronic device and the mobile application. This innovation attempts to regulate dog feeding appropriately and healthily by giving each dog the amount of food they need in accordance with their daily energy demands. In order to determine the daily ration of healthy and balanced food in accordance with daily energy needs, a nutritional evaluation of the dog's diet has also been undertaken, taking into account various parameters such as the dog's size, breed, and weight. The electronic gadget essentially consists of two parts: on the one hand, the electronic design is formed with an Arduino board, a Sim900 module to send and receive text messages, and the ESP8266 Wi-Fi serial transceiver module, which enables setting up an internet connection to receive tweets that users post. Both modules allow remote communication with the gadget using the Arduino board. As opposed to this, the Android-based mobile application uses a uniform design that complies with Google's material design principles. It enables the owner to feed, schedule the feeding, review the dog's food history, and get alerts when the food is about to run out.

Keywords:- Arduino, 5G Networks, Security and Framework

# 1. INTRODUCTION

Since the phrase was originally used by Kevin Ashton in 1999, the Internet of Things (IoT) has seen a number of technical advancements. Numerous scientific advancements and the automation of numerous processes have solved challenging business and societal issues and produced ground-breaking new goods and services. In the past ten years, industry, academia, and research have all focused on improving daily activities and creating new goods and services. IoT is a trend in current technological advancement. It is possible to develop new applications that lead to opportunities in various spheres of society and the economy. With the help of IoT technology, a situation is presented in which any physical object can be transformed into a terminal connected to the Internet in a domestic setting, allowing for the remote monitoring and control of various things from anywhere at any time. In order to be able to gather, analyse, and process data on computer platforms, different devices must be connected to one another and can be controlled remotely from anywhere, anytime, by anything, and by anyone [1]-[5].

As was already mentioned, there aren't many studies on automatic dog feeders. The current studies, however, rely on automatically feeding participants without considering the daily food intake in relation to the RDI and the maximum nutritional values. Therefore, a nutritious and balanced food is required in accordance with the daily energy needs for the dog to enjoy excellent health is shown in Figure 1. To that end, a nutritional evaluation has been carried out in this study, taking into account several elements such as the dog's size, breed, and weight to determine the daily ration of nutritious food in accordance with daily energy needs [6]-[10].
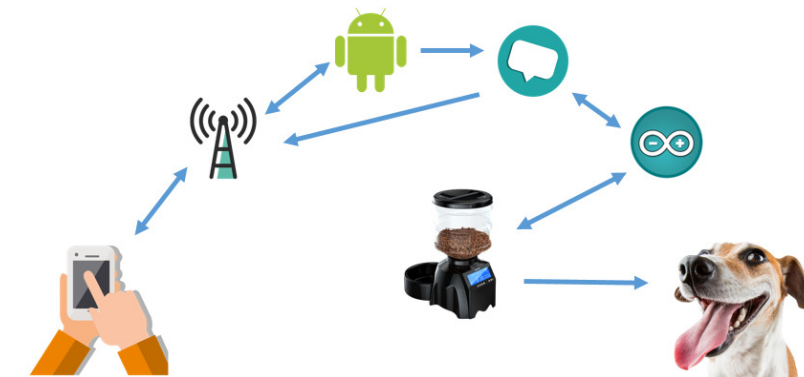


Figure.1. IoT Technologies

## 2. IOT WITH ARDUINO

The development of technological devices is currently possible on a variety of low-cost platforms, including Arduino [Arduino, 20], Raspberry Pi [Raspberry, 20], OpenPicus [OpenPicus, 20], Cubieboard [Cubieboard, 20], and Udoo [Udoo, 20], among others. The properties of each platform have been thoroughly analysed; the most popular and well-known are Arduino, OpenPicus, and Raspberry Pi. The Arduino platform is the main focus of this work, while for communications, GSM/GPRS technology and the social network Twitter have also been utilised. Finally, the mobile application is created using the Android operating system. Six of the 13 input/output ports on the Arduino board, which is based on the 8-bit ATMEGA328 microcontroller, can be set up as outputs to handle Pulse Width Modulation (PWM) signals. It has a six-channel analog/digital converter module and one UART port. It features a 2KB EEPROM memory unit and a 32KB programme flash memory [Pathak, 17]. It has some advantages over other platforms, such as being multi-platform, having an easy-to-understand programming

language, inexpensive boards, and open-source hardware and software [Arduino, 20]. The Global System for Mobile Communications (GSM) is a time division multiple access-based mobile communication system. General Packet Radio Service (GPRS) is a technology that uses packetized data transmission and operates more effectively than GSM while operating in the same frequency band [11]-[15]. The minimum data transmission speed for GSM is 9.6 Kbps, and the minimum and maximum data transmission speeds for GPRS are 40 Kbps and 115 Kbps, respectively [Wenzheng, 07] is shown in Figure 2.
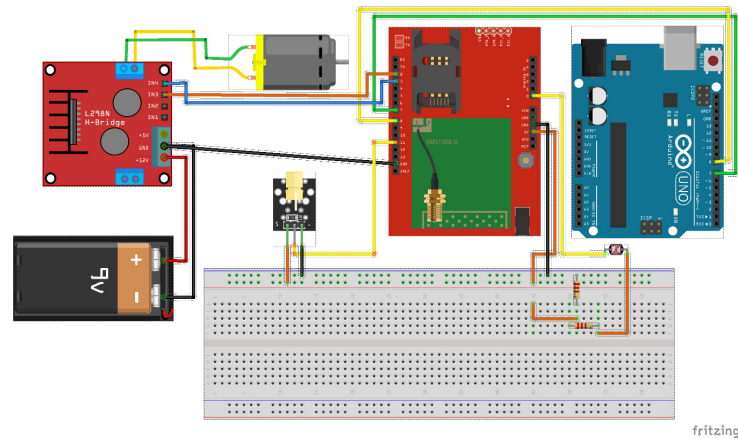


Figure.2. IoT with Arduino Board

Every Wireless Sensor Network is built on autonomous wireless sensors (AWSs) (WSN). Using current AWS technology, a wide variety of IoT-based applications may be created, including those for the military, biotechnology, business, and education. Structure, functionality, and application requirements are the major determinants of AWS energy optimization. All of the aforementioned aspects are addressed by the holistic design technique. In this regard, we provide an unique architecture-based approach that replicates both the power supply and the transceivers utilising a hybrid storage system. An suitable approach for sizing and managing the power flow for the power source is suggested by determining the consumption requirements of the transceivers. Through a series of transceiver testing scenarios, the article highlights the integration of information, communication, and energy consumption of the AWS in terms of spectrum information, highlighting the key variables that affect the design of the sensor nodes and their interdependencies. By including an energy-harvesting component in the sensors, system optimization takes into account all of these elements to create an AWS that uses less energy. Autonomous wireless sensors have made it possible to create intelligent and context-aware applications in many locations (rural, urban, and industrial) in the present Internet of Things (IoT) context (AWS). The Wireless Sensor Networks' essential component is autonomous wireless sensors (WSN). They must display high energetic performance, high data delivery reliability, and autonomy. The creation of a broad range of sensor-based applications in several domains, from the military to biotechnology and from industry to education, is made possible by current technology. In an exceedingly complex environment, the increasing complexity of the sensors' behaviour creates additional problems in terms of dependability, availability, accuracy, energy consumption, security, and data transmission efficiency. Due of this complexity, simulation test beds have been created to aid in making decisions on the hardware and software architecture of the next AWSs. It is crucial to determine the variation range and cross correlation of each

AWS parameter with other parameters. The AWS architecture makes reference to components and how they are organised, illuminating assumptions about subsystems. As a result, when it comes to power sources, the storage system must simultaneously meet the needs of both the application's fundamental power needs and its short-term power fluctuation needs. The decision about the transceiver and the protocol it is equipped with will be mostly influenced by the informative element.

Data acquisition coordination and AWS activity control, including the sampling control of the telegrams for ADC, are controlled by a micro-controller from the AVR8 family. By adding battery current sensors based on the Hall Effect into the supplying circuits of each transceiver, the working current is determined. These provide a signal that is proportionate to the current that the AWS's transceivers are absorbing. The sensors have an operating frequency of 50 kHz and a 0.2% accuracy. The current signal from the supplying circuits of the two AWS transceivers is observed by an analogue multiplexer included within the AWS controller. An I2 C interface connects a secondary ADC with a 16-bit resolution and a 15-sps sampling rate to the AWS controller. The auto-calibrated 16 bit ADC ensures the translated signal's excellent precision in a variety of environmental circumstances. This enables the capture of extra signals at low sample rates and high resolution. The signal obtained determines the sampling rate of the temperature and humidity sensors (14 bits for temperature and 12 bits for relative humidity). Temperature input ranges from 40°C to 125°C, while relative humidity input ranges from 0% to 100%.

We developed the system employing two transceivers (BLE and RFM—2.4 GHz) to study the possible benefits of communication hybridization employed for AWS sensors. The suggested AWS approach seeks to reduce consumption while simultaneously increasing the network's potential AWSs' range and quantity. Short-range (up to 10-30 m) and medium-range (400-1000 m) wireless communications are made possible by the two transceivers employed. An UART and an SPI serial interface are used by the AWS's main CPU to manage these operations. This study helps us comprehend the new super-capacitor-based architecture used by AWS for its quick release supply. We looked into and calculated a number of information flow and energy efficiency-related factors. Therefore, the lifespan, dependability, and availability of the AWS will be influenced by information heterogeneity and the power provided. So, by adjusting immediate parameters, the addition of super-capacitor parts results in gains in energy efficiency (current, voltage, and power). Energy harvesting from the environment is feasible from the standpoint of the power supply. Power continuity for the AWS must be provided by the fast storage component. However, the transmission of information results in large changes in the demand on the power supply that may be offset by the use of super-capacitors. Benefits include avoiding battery stress, which lowers internal power supply resistance and enhances transceiver transmission. Future research will investigate these features' specifics. Additionally, by taking into account technical advancements in the condensed matter field, we want to examine the integration of rapid storage components within the transceiver.

3. COMMUNICATION NETWORKS

We have IoT on a variety of levels, including the interface layer, the service layer, the network layer, and the sensing layer. The network layer is the layer above the sensing layer, and it is responsible for sending data that

has been detected, gathered, and communicated to other layers further up. Sensor networks, social networks, many other networks and data bases, the internet, and other systems are primarily served by the network layer. The network layer is that. We have the service layer, which primarily deals with the delivery of services, including service integration, service division, service repository, service logic, and business logic. All these varied things have developed as a result of the services being offered to assist various corporate tasks. Next, we have the application frontend, contract interface, interface layer, and application APIS. When we have security vulnerabilities, which essentially cross all of these various layer horizontals, this becomes the interface layer. Fog computing is a new system architecture that is being used recently, where sensors and network gateways do some of the data processing and analytics. The monitoring, pre-processing, storage, and security layers are inserted between the physical and transport levels in a tiered manner via a fog architecture. Power, resources, replies, and services are all tracked by the monitoring layer. Filtering, processing, and analytics of sensor data are carried out by the pre-processing layer. Data replication, dissemination, and storage are just a few of the storage capabilities offered by the temporary storage layer is shown in Figure 3. The security layer also assures data integrity and privacy and conducts encryption and decryption. Before transferring data to the cloud, monitoring and pre-processing are carried out at the network's edge.
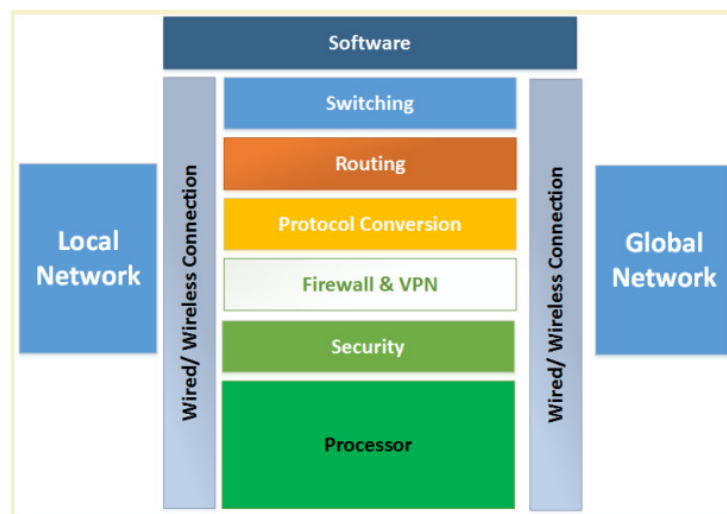


Figure.3. Architecture of IoT with Wireless Networks

IoT basically depends on a number of key technologies to survive. Through data assignation, data collection, processing, and analysis, we have the future internet knowledge aggregation. Additionally, we have a variety of standards, sensor networks, communication, cloud computing, discovery services, embedded systems, software system integration, nano electronics, and, last but not least, security and privacy concerns. Because we are dealing with resource-constrained nodes with communication constraints, bandwidth constraints, processing constraints, and energy constraints, security and privacy concerns are pervasive in the Internet of Things. Because IoT systems are so detailed-intensive, there is a lot of information that flows through the network, putting the privacy of the people and the organisations at risk. As a result, these nodes become extremely valuable to various attacks and security breaches. As a result, IoT technologies rely heavily on security, privacy, and trust, all of which

are not mentioned here. Transport for Message Queue Telemetry. As a result, it is an ISO standard that uses the publish-subscribe business model. So, in essence, you already know what happens: data is published in some way, and then subscribers download it. So, this is how the publish-subscribe model operates, and what MQTT has essentially done is make the publish-subscribe model lightweight by using this protocol, allowing it to be used in conjunction with the TCP IP protocol suite. What MQTT supports is this. According to its history, IBM first introduced MQTT in 1999, and Oasis standardised it in 2013. It has been standard since 2013. Therefore, this particular protocol accomplishes a few goals. One is providing connectivity between various embedded devices so that applications, middleware on one device, and network and communication on the other device can all communicate with one another. So, on the one hand, we have connection between applications and middleware, and on the other, we have networks and communication

Science and technology working together have made it possible to create tools and technologies that make everyday tasks simpler. Today, technology is a basic benchmark in every application field. The creation of new goods and services and the enhancement of daily activities have drawn the interest of business, academia, and research over the past ten years. Numerous technological advancements have been made for a variety of personal applications, including those at home, in the workplace, in education, and in organisations. The manufacturing sector is no exception to this rule given how popular it has grown to be. Two communication architectures have been presented in this work as an alternative to feeding animals, particularly dogs. The use of Twitter and the GSM/GPRS communication services has made it possible for owners to remotely control and monitor feeding from any location at any time. Additionally, it enables the timing to be determined and the recommended ration to be given based on the dog's weight. Additionally, it has alerts that send reports on feeding times and alert the owner when the food is about to run out. The creation of this electronic device aims to regulate the feeding of the dogs in accordance with their daily energy needs. In this sense, a thorough examination of the dogs' recommended daily intake as well as a systematic evaluation of the amount of metabolizable energy in dog food were conducted.

Both architectures can establish remote communication at any time and anywhere, based on the results obtained. The establishment of the communication, however, depends on the coverage of the mobile network when using GSM/GPRS communication services through the Short Message Service (SMS). To send SMS and complete the feeding process, the device's SIM card needs to be activated with a phone plan or rechargeable cards. Otherwise, a wireless internet connection where the electronic device is located is required in order to establish communication through the ESP8266 Wi-Fi serial transceiver module when using the Twitter social network. Once a connection has been established, all that is required to continue communicating is to send a tweet using any Internet-connected device from the Twitter user account. As was previously indicated, both communication architectures are functional nowadays due to the widespread use of mobile networks and the fast data transfer rates offered by Internet services is shown in Figure 4. A drawback of the GSM/GPRS communication architecture is that it restricts the usage of the electronic gadget to the mobile phone on which the application is loaded; if the phone is misplaced or forgotten, feeding cannot be done. When    tilizing the social network Twitter, this restriction is not an issue since all that is required is for the owner to check in from any computer or mobile device with an Internet connection.
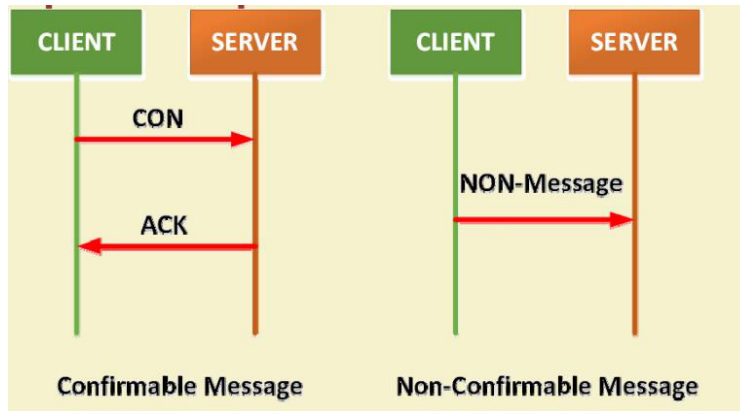
Figure.4. Acknowledgement

It is crucial to keep in mind that innovation in logistics typically does not fundamentally alter the industry but rather allows for improving process efficiency or enables new value-adding features. The first conclusion that can be drawn from the discussion that has just taken place is that the warehouses will eventually become fully automated, with items being checked in and out and orders being sent to the suppliers automatically. Better asset management and proactive planning on the part of the carrier will be possible as a result. Goods may be transported from producer to consumer without human intervention, and manufacturers will receive immediate feedback on the demands of the market. This allows for the dynamic adaptation of production and transportation, saving time, energy, and the environment. Executable code embedded in the tags enables the object in transit to make wise routing decisions based on data obtained from readers or positioning systems. By doing so, the item's forwarding can be optimised, and the manufacturer or the customer will be given control over the routing instead of the transporter. The item may recheck with the sender to determine whether it should proceed to the intended recipient or move to another recipient who will pay more quickly for the item. Modern logistics is based on supply chains that have been in place from manufacturer to consumer. Legally binding supply chains that have been in place for a while. It is conceivable to think of the things in motion as a marketplace where a consumer could post a request on the Internet of Things, get an offer from a thing that can fill it, and accept it. An assembled thing might be built from parts automatically identified on the Internet of Things, similar to service composition in the virtual software world where an application is assembled of various services available on the Internet. This will alter how business deals are made because customers might not order a large quantity of goods from a manufacturer but rather purchase them sequentially from different manufacturers, possibly at competitive prices. Depending on the IoT applications being used, various sensing nodes are required. A camera system for image monitoring, water or gas flow metres for smart energy, radar vision for active safety, RFID readers for object or person detection, doors and locks with open/close circuits that indicate building intrusion, or a basic thermometer for temperature measurement is examples of sensing nodes. The bottom line is that, depending on the applications, there may be numerous different types of sensing nodes. Each of these nodes will have a distinctive ID and be individually controllable via a remote command and control structure. There are use scenarios where a smartphone equipped with RFID, NFC, and/or GPS capabilities may approach certain RFID/NFC-enabled "objects" in a structure, connect with them, and record their precise

positions on the network. Therefore, remote registration and, eventually, command and control of the IoT, will use RFID and NFC.

4. CONCLUSION

As we already mentioned in the introduction, society's decisions are dynamic and based on knowledge of the issues and experiences with technology. Technology research alone cannot determine the balance between security and privacy; instead, societal interaction is required. However, as the results of research have demonstrated, technology can help achieve a better balance between security and privacy, for example by enabling the restriction of communications to those portions of data sets that are currently required. For the purpose of addressing security and privacy, we proposed an approach based on the SecKit in this book chapter, in which policies can be used to control the flow and access of user data. Giving the user control over his own data is a benefit of this strategy. The limitation of the approach is that the quality and potential ambiguity of the sensor data collection is not addressed in the perception of the context taken into account. Future framework developments will address this aspect, which is actually based on the precise definition and detection of the context. The adopted scenario also only involved a small number of entities, whereas in the IoT of the future, each IoT device will need to communicate with many different interfaces. We will look into cloud computing and cluster approaches, as well as partitioning the monitoring function to reduce data flow and computation overhead, to address this final scalability-related issue.

REFERENCES

[1] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian,"Mina: A reflective middleware for managing dynamic multinetwork environments," in Proceedings of IEEE/IFIP Network Operations and Management Symposium 2014, ser. NOMS 2014. Krakow, Poland: IEEE, 2014.

[2] A. Sydney, "The evaluation of software defined networking for communication and control of cyber physical systems," Ph.D. dissertation, Department of Electrical and Computer Engineering College of Engineering, KANSAS STATE UNIVERSITY, Manhattan, Kansas, 2013.

[3] Y. Yiakoumis, K.-K. Yap, S. Katti, G. Parulkar, and N. McKeown, "Slicing home networks," in Proceedings of the 2nd ACM SIGCOMM workshop on Home networks, ser. HomeNets '11. New York, NY, USA: ACM, 2011, pp. 1–6. [Online]. Available: http://doi.acm.org/10.1145/2018567.2018569

[4] T. Luo, H.-P. Tan, and T. Quek, "Sensor openflow: Enabling softwaredefined wireless sensor networks," Communications Letters, IEEE, vol. 16, no. 11, pp. 1896–1899, November 2012.

[5] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, "Devoflow: scaling flow management for high-performance networks," in Proceedings of the ACM SIGCOMM 2011 conference, ser. SIGCOMM '11, 2011.

[6] M. Al-Fares, S. Radhakrishnan, B. Raghavan, N. Huang, and A. Vahdat, "Hedera: dynamic flow scheduling for data center networks," in Proceedings of the 7th USENIX conference on Networked systems design and implementation, ser. NSDI'10, 2010.

[7] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," SIGCOMM Comput. Commun. Rev.

[8] M. Mendonc¸a, B. N. Astuto, X. N. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," 2013, in Submission In Submission. [Online]. Available: http://hal.inria.fr/hal-00825087

[9] Chen H., Finin T., Joshi A., Kagal, L., Perich, F. and Chakraborty D., Intelligent agents meet the semantic web in smart spaces, IEEE Internet Computing, vol. 8, no. 6, pp. 69 – 79, nov.-dec. 2004.

[10] Gessner, D.; Olivereau, A.; Segura, A.S.; Serbanati, A., "Trustworthy Infrastructure Services for a Secure and Privacy-Respecting Internet of Things," Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, vol., no., pp.998,1003, 25-27 June 2012.

[11] Huang X., Fu R., Chen B., Zhang T., Roscoe, A.W., User interactive Internet of things privacy preserved access control, Internet Technology And Secured Transactions, 2012 International Conference for , vol., no., pp.597,602, 10–12 Dec. 2012

[12] ISO/IEC 24760-1:2011 Information technology—Security techniques— A framework for identity management—Part 1: Terminology and concepts.

[13] Pohls H. et al., "Rerum: Building a reliable iot upon privacy- and securityenabled smart objects," in Proc. of WCNC, 2014.

[14] Neisse, R. Trust and privacy management support for context-aware service platforms. PhD thesis, University of Twente. CTIT Ph.D. Thesis Series No. 11–216 ISBN 978-90-365-3336-2.

[15] Vlacheas, P.; Giaffreda, R.; Stavroulaki, V.; Kelaidonis, D.; Foteinos, V.; Poulios, G.; Demestichas, P.; Somov, A.; Biswas, A.R.; Moessner, K., Enabling smart cities through a cognitive management framework for the internet of things, *IEEE Communications Magazine,* , vol.51, no.6,pp.102,111, June 2013