
Article:
Umer, T., Rehmani, M.H., Kamal, A.E. et al. (1 more author) (2019) Information and resource management systems for Internet of Things: Energy management, communication protocols and future applications. Future Generation Computer Systems, 92. pp. 1021-1027. ISSN 0167-739X

https://doi.org/10.1016/j.future.2018.11.032

Information and Resource Management Systems for Internet of Things: Energy Management, Communication Protocols and Future Applications

Tariq Umer, Senior Member, IEEE, Mubashir Husain Rehmani, Senior Member, IEEE, Ahmed E. Kamal and Lyudmila Mihaylova

***Abstract*—The idea of the Internet of Things (IoT) has enabled the objects of our surroundings to intercommunicate with each other in diverse working environments by utilizing their embedded architectural and communication technologies. IoT has provided humans the capability to manipulate the operations and data available from different information systems using these intelligent objects available in the surroundings. The scope of IoT is to serve humanity across different domains of life covering industrial, health, home and day-to-day operations of Information Systems (IS). Due to the huge number of heterogeneous network elements interacting and working under IoT based information systems, there is an enormous need for resource management for the smooth running of IoT operations. The key aspect in IoT implementations is to have resource-constrained embedded devices and objects participating in IoT operations. It is important to meet the challenges raised during management and sharing of resources in IoT based information systems. Managing resources by implementing protocols, algorithms and techniques are required to enhance the scalability, reliability and stability in IoT operations across different fields of technology. This special issue opens the new areas of interest for the researchers in the domain of resource management in IoT operations.**

***Index Terms*—Internet of Thing (IoT), Resource Management, Energy Management, Communication Protocols.**

I. INTRODUCTION

The advancements in Internet technologies have given the new aspects of controlling and managing daily operations of devices in our surrounding using wireless technology. In the new era of information technology, these emerging technologies are converging to support and enhance the human standards of living. The integration of sensors and Radio-Frequency Identification (RFID) with machines has enhanced their capability to react, behave and operate as intelligent autonomous bodies. These developments have given a new vision for researchers to implement the idea of smart working and smart living environments across different domains of life. The Internet of Things (IoT) provides the interconnection of objects implanted with sensor and communication technology to work under diverse working conditions. It enables its users to manage their day-to-day operations and gain useful data to serve humanity. IoT is an effort made by researchers to develop a communication platform for the devices, which is supported by hardware and communication technologies. This platform when implemented in devices, provides the capabilities of intercommunication and interoperability. The ongoing progress in different fields of technology matures the idea of IoT to such an extent that it becomes a hot issue for the research community. The survey [1] summarizes the different aspects of IoT development. The study presented the evolution of IoT and defines the idea as an accomplishment of the human dream to have the ability to sense the physical world and objects of our surrounding. The availability of RFID and Wireless Sensor Network (WSN) technology gives the roadmap for the establishment of smart environments which leads to the implementation of IoT concept.

The scope of IoT was defined to design a new class of applications to achieve smart working environments for living. It is focusing on providing the capability to control and manage the objects in their surroundings. To establish these conditions it is desired to have a set of standards and well-defined working conditions for IoT. A comprehensive survey [2] discussed the role of fundamental technologies in IoT implementation and operations. The study summarized the working of developed protocols applied during the operations of IoT. The interrelationship between the different domains where IoT is broadly applied is also provided. This gives the understanding of IoT operational requirements for devices needed in intelligent decision making against defined objectives.

To present the trends in IoT implementation, operations and management the study [3] analyzed the research contributions on the issue of IoT across different well-known journals. The analysis is carried out on the basis of some classification considering key parameters of hardware, technology, applications, business models and challenges. The study gives the future working directions on open research issues such as IoT diffusion, context-aware and ambient intelligence in IoT. Another key feature of IoT vision is to provide enhanced working environments for different industrial and manufacturing units. To highlight the IoT based products and services available for different enterprises an effort is made in [4]. To meet the technical issues and challenges during the provision of IoT services for diverse industrial environments, IoT applications

Tariq Umer is with Department of Computer Science, COMSATS University Islamabad, Wah Campus, 47040 Wah cantt, Pakistan E-mail: (t_umer@yahoo.com)

Mubashir Husain Rehmani is with Waterford Institute of Technology (WIT), Ireland Email:(mshrehmani@gmail.com)

Ahmed E.Kamal is with Department of Electrical Engineering, Iowa State University, USA. Email:(kamal@iastate.edu)

Lyudmila Mihaylova is with University of Sheffield, Sheffield, UK Email:(L.S.Mihaylova@sheffield.ac.uk)

Manuscript received Month 00, 2017; revised Month 00, 2017.

are categorized in three main areas; covering monitoring and controlling of operations, gaining and managing big data and providing business analytics and enabling information sharing and collaboration. The study also explores the investment opportunities in the area of IoT based industrial revolution considering the customer values. IoT has enabled the objects of our physical world to interact, probe and communicate with each other under diverse working conditions. The availability of virtual objects, their roles, issues and suitable platforms to implement the concept of virtualisation in these IoT communications is presented in [5]. The survey presented the comprehensive overview of the characteristics, architecture, functionalities, and issues during the implementation of virtual objects in IoT operations.

Multimedia services and applications hold a significant share in day-to-day operations and data transfer of communication networks. To extend the role of multimedia objects in IoT a review article by [6] gives the idea of the Internet of Multimedia Things (IoMT). The proposed architecture of IoMT enables heterogeneous multimedia things to interact and operate in a collaborative environment. The presented architecture for IoMT operations is based on the parameters of sensing, addressing, cloud and multi-agent system at four different layers. The available technologies, issues and future research directions are systematically discussed in IoMT perspective.

The fusion of IoT with different technologies opens doors for the researchers to consider different aspects of IoT for future extension and its dynamic implementation. The ref [7] carried out a comprehensive survey, focused on the role, working, standards and implementation of context-aware computing with IoT. The study analyzed a large number of projects in the area of context-aware computing and gives a guideline for future evaluation of IoT implementation under context-aware paradigm. To elaborate the role of technologies, protocol and applications in IoT operations the authors in [2] presented an overview on the relation, impact and characteristics of these parameters across different domains of human life and gave a guideline for the future implementation of IoT.

In the remnant of the paper, we present the framework required to implement IoT. The key areas of framework suggested as Supporting technologies for IoT operations, Routing protocols, Business models and Operating system are presented in Section II. An overview of the accepted papers in the domain of Energy management, Routing strategies, Securing techniques and Cloud based application in IoT is given in Section III. Finally, the Section IV concludes the paper.

II. IoT IMPLEMENTATION FRAMEWORK

As the idea of IoT is gaining more and more maturity, the number of participating devices, platforms and applications will grow tremendously in the near future. Due to the heterogeneity of these devices platforms, implementation scenarios and applications a common set of rules and operating procedures are need to be defined. To overcome the gap between the different working layers of IoT, joint efforts are made by variuous networks governing bodies, forums and researchers to introduce standardization for IoT implementations. The researcher in [8] summarized the work carried out by Standards Development Organizations (SDOs) such as IETF, ITU-T, ETSI, ISO/IEC and IEEE for introducing standardization and policy guideline for the researcher, industry and governments for the smooth running and monitoring of IoT operations and mechanisms. These efforts will bring fairness, mutual cooperation and healthy competition among all the stakeholders of IoT. The ref [9] highlighted the contributions and efforts made by different organizations in standardizing the operations of IoT in Machine-to-Machine environments.

To meet the requirements of IoT implementation a modular approach is adopted by the researchers to define the components. They have presented a five-layer architecture which defined the working boundaries of different IoT technologies, protocols and applications. In these working models, every individual layer takes care of its defined working procedures and provides outcomes for IoT system. The five layers are performing different operations. The first object layer is dealing with physical components and their characteristics such as sensors and actuators functionalities, the object abstraction layer residing between object and service management layer is managing data transfer between these two layers using available technologies, the third service management layer deals with naming, addressing and data delivery issues between heterogeneous platforms of IoT, the application layer interacts with the users and provides useful information as requested by the customers. The last business layer controls the activities, operations, application and overall management of IoT system elements. To provide the clear understanding of the functionalities and working procedure of IoT, the research studies also defined the key elements of IoT system named as device identification, sensing and communication technologies, computation capabilities, available services and semantics. These elements are working together to achieve a collective objective of IoT using different technologies, protocols, operating systems and business models [2] [10]. The deployment of sensory devices in home environments instigated the concept of IoT for home users. To manage and control the IoT services in heterogeneous IoT home networks a management framework is presented in [11]. The proposed model evaluates the important constraints of gateway bottleneck and local services management by using ECHONET LITE devices under Constrained Application Protocol (CoAP). To maintain a web-based scheduling of IoT applications, a service-oriented architecture using scriptable agent named as ScriptIoT is suggested in [12]. The result achieved in the study shows more flexibility and scalability in access time and CPU scheduling during large-scale application deployments.

A. *Technologies Supporting IoT Operations*

The architecture of IoT is divided into multiple functional layers. Different technologies are designed to support IoT operations on these layers. To achieve secure and reliable end-to-end data delivery different constraints, mechanisms and elements are defined by these technologies at each layer. These technologies are merged to play an important role in providing

services as required by their respective layer operations [10], [13]. These technologies are divided into four function layers as discussed below :

*1) **Data Acquisition Technologies**:* In IoT implementation, the key aspect is to gain all important data from the connected devices. The gathered data is forwarded to the application which processes it into useful information for the users. During the IoT operations, data acquisition stage is responsible to receive and forward data through signals to the relevant application using data acquisition technologies. There are three major data acquisition technologies having unique characteristics which enable their implementation in diverse environments. The key focused technology in IoT for data acquisition is Radio Frequency Identification (RFID). It is a wireless automatic identification technique, which uses radio frequency signals to obtain messages from nearby devices. The RFID system required an electronic label, a reader and a supervising computer. An RFID system is used due to its many advantages. It has the ability to provide anti-interference, a larger amount of information with good visual range and reading-writing scope having longer usage life. Compared to barcodes, in RFID the data is stored on an electronic label in the form of a radio frequency card or non-contact IC card. It consists of a label chip with circuits inside and an antenna. Two types of electronic-labels are available in RFID: passive and active. A passive RFID consists of a dependent power supply meaning it receives power from the computer. On the other hand, the active RFID operates on battery. Active RFIDs are more costly, larger sizes and have shorter lifespan than passive RFIDs; however active RFIDs have greater storage capacity and long-range capabilities.

An RFID reader consists of a transmitter, a receiver, a microprocessor, memory unit, input/output channels, actuators and annunciators, a controller, a communication interface, and a power supply. RFID is a form of data communication between devices in IoT. It is a prevailing technology, used by numerous manufacturers. Hence adequate standards exist to ensure proper installation in IoT environments.

Another largely implemented data reading technology from devices is a Two-dimensional code. A key element in this technology is a barcode. A barcode provides a visual means for the representation of data that can be read and obtained using a barcode reader machine. One-Dimensional codes store data using the widths and spacing of horizontal parallel lines. Their disadvantages are that they can only represent letters and numbers. Their opertion needs to have a back-end database. This results in a smaller storage capacity. Hence two-dimensional codes were developed. The two-dimensional codes use black and white pixels for representing data. The black pixel represents binary "1" and white representing binary "0". Two-dimensional codes have many advantages such as high storage capacity, high reliability and the aptitude to express various forms of information (sound, graphics, text, numbers etc.). Two-dimensional codes have the capability to read the data even when the barcode area is damaged up to 50. 2D barcodes are generated using algorithms. Machines then read the two-dimensional barcodes and an image sensor processes them. A computer accesses the processed data and displays the results [14].

In comparison with two-dimensional barcodes, RFID has a major advantage due to its potentials of operating without human contact. RFID tags can perform hundreds of operations per second without assistance. RFID tags attached on a product can be rewritten, reused or switched off; barcode readers, on the other hand, do not have this feature. RFID tags can hold more information, do not wear-and-tear and are not affected by dirt and dust especially in a large number of devices deployment in IoT [15], [16]. A single microchip board platform integrated with sensor, communication module and security features provides capabilities to the device, to serve as an active member in IoT environment. Keeping in view the operating conditions and working environments around humans, sensors are specially designed to sense and gain data under specific conditions such as bio-sensors are designed for gaining biological data, solid-state image sensors work under light and electronic signal environments, thermal flow sensors provide data from thermodynamic parameters such as heat sensing devices inside buildings to provide information about working conditions and structures in smart cities environments. In the process of sensing, the required data is acquired according to the capability of the installed sensor. The gathered data is then forwarded to the centralized management station for further processing according to the required services [17], [18].

*2) **Data Processing Technologies**:* In IoT extensive amount of data processing is performed to run the user level applications operations. To gain these capabilities, hardware-based solutions and technologies are designed for IoT environments. In hardware level processing a key aspect is to provide high-speed processing platform which can provide fast, reliable and energy efficient data processing in diverse working conditions. To fulfil these requirements various platforms are designed by the industry such as Arduino, FriendlyArm, Intel Galileo, Raspberry PI, Gadgeteer, BeagleBone, Cubieboard and WiSense etc [1], [10], [14]. These platforms provide high-speed computation and data management capabilities using cooperative and efficient co-processing techniques.

*3) **Data Storage Technologies**:* Due to a large number of connected devices and running applications, a huge amount of data is produced by IoT environments. To achieve a high level of reliability and accessibility of data, the data management and composition at device and server level is very critical. The algorithms based on artificial intelligence and machine learning techniques are designed to have smart monitoring and efficient operational management in IoT [18].

*4) **Data Communication Technologies**:* In IoT, it is important to perform timely distribution and accessing of collected data from the devices to the applications. Due to the presence of heterogeneous devices the communication channel in IoT is prone to be very noisy. The availability of communication technology providing more energy efficiency, reliability and scalability are required in IoT environments.

To meet these goals a number of communication technologies are implemented for supporting IoT operations. RFID, Near Field Communication (NFC) and Ultra-wide bandwidth (UWB) technologies are designed to enable the short distance communication between the connected devices. The devices are able to communicate between the ranges of 10cm to 200m in RFId and up to 10cm in NFC using frequency band of 13.56 MHz with the support of 424 kbps data rates. Both technologies are implemented using a special purpose identification tags. These tags installed on devices serve as data receiver or sender unit in communication. In UWB the communication channel provide high data rate with low energy utilization in communication using attached sensor on the devices [19], [20]. To support the large range of communication in the device to device environment IEEE have also introduced standards for IoT. These standards are IEEE 802.11(WLAN), IEEE 802.15.4 (Zigbee), IEEE 802.15.1 (Bluetooth) whereas the standards such as WirelessHART, WiFiDirect, Z-Wave and IETF 6LowPAN are based on IEEE 802.15.4 standard. The key objective of these standards was to enhance the communication channel capabilities in IoT implementations with high bandwidth, extended communication range and low power consumption during device to device communication. These standards are designed to support all IP based networks such as IPv4 and IPv6 networks [21], [22].

B. Role of Protocols in IoT

During the operations of IoT large number of embedded devices communicate with each other and generate a huge amount of traffic. In IoT environments, these devices are designed to consume less power and operate more efficiently. Efforts were made by different standardization organizations to develop a standard protocol stack having characteristics of low power usage, reliability and efficient communication capabilities. The availability of multi-vendor products in IoT environments require common standard which can provide interoperability and resiliency across these platforms. The standardization bodies IEEE and IETF had put their efforts to build a protocol stack to support communication in IoT. The protocol stack designed for IoT environments performs operations from physical to the application layer. Several working groups are formed to design protocols to meet the requirements of specific layer [23]. The key working groups and their contribution in protocol design are discussed as under:

1) ***IPv6 over Low Power WPAN (6LoWPAN)****:* In IoT environments, IPv6 addressing scheme is implemented to support a large number of devices. An IETF 6LoWPAN working group is established to provide interconnection between IPv6 based nodes and link layer technology IEEE 802.15.4 in IoT environments. The low power wireless networks hold unique characteristics such as small packet size, variable length address, low powered and low-cost battery-operated devices and unpredictable working conditions. To provide a mapping between the services of IPv6 and link layer technologies 6LoWPAN working group introduced an adoption layer. The new working layer performs header compression, fragmentation and logical grouping to meet the IPv6 transmission requirements. In 6LoWPAN standard different frame headers are defined to manage communication at the network layer. The NO 6LoWPAN header is designed to manage and discard the packets which do not comply with 6LoWPAN specifications. A Dispatch Header is introduced to compress an IPv6 header and control multicast/broadcast from link layer. To convert IEEE 802.15.4 frames from single-hop WSN to multi-hop environments a Mesh addressing Header is implemented in adaption layer. A Fragmentation header is used to manage oversized frames in IEEE 802.15.4 and 6LoWPAN intercommunication [24]

2) ***Routing Over Low Power and Lossy Networks (ROLL)****:* IoT operates under diverse conditions and holds the characteristics of low power and lossy networks. It faces these conditions due to the dynamic topology changes and nodes status changing with respect to power condition and heterogeneousness of the nodes. A working group known as Routing Protocol for Low power and Lossy Networks (RPL) is designed by IETF to support data forwarding in these low powered and lossy networks. RPL is designed to support IPv6 address with link-independent routing. It provides data forwarding for the resource-constrained nodes implemented in industrial, urban and home automation environments. As the devices in IoT are interconnected in a mesh topology, a routing strategy is required which can supports interconnectivity such as multipoint-to-point, point-to-point and point-to-multipoint under lossy links. The operations of RPL are based on the formation of Directed Acyclic Graph(DAG). In these graphs, different root nodes are defined by having more Destination Oriented DAGs (DODACs). By using an Objective Function (OF) the rank of each node is calculated, which defined the number of metrics and constraints required by the root node for path calculation in low power and lossy network. To maintain the routing updates between the nodes RPL use four types of the message during its operations. These messages provide information regarding DODAG status and working conditions during routing in IoT. The DODAG rank information is provided by DODAG Information Object (DIO) message type. A Destination Advertisement Object (DAO) message type is used to achieve upward and downward traffic information of the selected node. To receive DIO information from adjacent node a DODAG Information Solicitation (DIS) message is implemented. For the acknowledgement of receiving messages and interaction between nodes, a DAO Acknowledgment (DAO-ACK) is designed in RPL [25].

3) ***Constrained Restful Environment (CORE)****:* To provide the embedded web services for the users of IoT an IETF working group, called as Constrained RESTful Environments (CoRE), was established to develop a suitable protocol which can support resource-oriented applications using RESTful embedded web services keeping in view the available technologies. The efforts of workgroup come out with a designing of new protocol known as Constrained Application Protocol (CoAP). The protocol holds the characteristics of RESTful web transfer with support for constrained networks and nodes. The CoAP structure is based on the same RESTful principle as defined for HTTP. To make the protocol more efficient and fast on constrained devices, it is designed lighter then HTTP and

use UDP protocol to reduce overhead and a small length of the header. Its message header is only 4 bytes which hold the information regarding version, type, token length, code and message ID. The CoAP operation is based on client/server model similar to HTTP. CoAP supports Multicast as well as Unicast [25].

C. Business Models in IoT Implementations

With the increasing understanding and maturity of IoT concept, the IoT based hardware, software and technologies are undergoing tremendous growth and enhancements. The dream of providing intelligence and communication capabilities to the devices and machines initiate thinking among the researchers and entrepreneurs to find possibilities, generate new services, create values to the products and finding new solutions of the business issues by merging IoT in daily ongoing activities. In organizational systems, devices and objects working under IoT implementation are resource constrained and interdependent on each other. Due to the availability of a large number of heterogeneous elements and multi-dimensional organizational activities, the implementation and operations of IoT based information systems, essentially required a framework, policies, working protocols and resource management in organizations. Managing of people, data and devices by having policies, protocols and algorithms play a key role to enhance the functionality, reliability and stability in the operations of IoT across the different domain of life.

To manage and coordinate between all the resources and activities in IoT based systems, international forums, standardization organizations, industry and researcher have highlighted the aspect of governance for these setups. It is required to bring all the activities under a well-structured framework which can define the users and stakeholders roles, responsibilities, limitations, competition and regularity approaches for a conducive working environment for IoT implementations in organizations and industries. Keeping in view the EU perspective, the research study [26] presented the key aspects of IoT governance. To have successful operational IoT infrastructure it is essential to focus on the issues of data privacy and protection, security and safety of the system elements, implementing policies for controlling ethical issues and managing interoperability of the objects. To support the IoT applications in business and industries research study have presented business models to define a framework for IoT implementations in these domains. The study [27] suggested a business model framework keep in view the IoT applications, The study conducted surveys, and interviews with all the stakeholders of different business and formulate a more effective business framework that consists of different building blocks covering important business parameters of partners, customer relationship, customer segments, channels, key activities, key resources, cost and revenue calculation and values propositions. With the growth of IoT implementation and applications, there is a need to bind entrepreneurs and potential users under an ethical framework which can define their responsibilities and moral duties to run and use the IoT based systems. The rules and procedures for the user interaction with IoT services and applications are defined in [28]. It suggests a policy-based framework that defines rules for the accessing of user data and services. To manage the user access in IoT environments the research study [29] summarized the issues and challenges for access control in home and enterprises based IoT environments. The survey gives the qualitative and quantitative evaluation of policies required to manage security and data access in IoT applications. In order to have control and management of services in IoT devices, a trust management is a key factor. The study [30] highlighted the four dimensions of trust including composition, propagation, aggregation and formation to understand the trust framework between the service provider and customer. The suggested framework define the security threats from internal and external factors due to the lack of trust management in IoT services and gives future research directions in this domain. The revolution of IoT has enabled it to support and work with different ongoing and emerging technologies. To explore the possibilities, potentials, and opportunities of IoT expansion under new emerging technology of 5G the study [31] analyzed the architecture and business models for IoT implementation under 5G. The impact on the relation between the vendors, operators and users in businesses is discussed under 5G technology in IoT.

D. Operating System

In IoT devices work under the constraint of limited power, computational capabilities and memory storage. To meet these limitations a well designed operating system (OSs)is required during the implementation and operations of IoT. A critical survey covering the different available operating systems on IoT is presented in [32]. The survey gives the comprehensive comparison of the characteristics and features of all available IoT operating systems. To support the concept of IoT under Low-End devices the authors in [33] presented the characteristics and capabilities of OS required for Low-End devices. The OSs need to support devices small memory, heterogeneous hardware architectures, network capabilities, efficient energy management and real-time operations of IoT devices. During the design phase of OSs, the technical capabilities should provide its architectural design, scheduling, memory allocation, network buffer management and programming model. The non-technical properties of OSs design focus on issues of standards, certifications, documentation, licensing and maturity of code and OSs service providers. To meet the requirements of the real-time application of IoT, the study [34]presented the overview on the characteristics of Real-Time Operating Systems (RTOS) designed for IoT. The operating systems have the capabilities to manage the operations of Embedded Systems (ES)implemented in IoT. RTOS operations are based on the priority based schedulers and manage operations in preemptive and non-preemptive modes. The usage of Software Defined Networking (SDN) in IoT is explored in [35] by introducing the concept of Open Network Operating System (ONOS) in IoT. The SDN is applied using SDN-WISE protocol for the operations of IoT using OpenFlow standard (OF) switches. To highlight the TinyOS trends and supported application in IoT a review is presented in [36]. The TinyOS is able to

support operations of IoT having limited resources, low energy and diverse working conditions. During the deployments of TinyOS in IoT different programming models are available for managing IoT operations. To highlights, the importance of OSs in the operations of IoT the [37] provides the comparative review of OSs design, scheduling methods, underline communication technologies, applied programming models and used power and memory methods.

III. A BRIEF REVIEW OF ACCEPTED ARTICLES OF THIS SPECIAL ISSUE

This special issue was focused to solicit the efforts and ongoing research work in the domain of resource management in IoT. The contributions in this issue are elaborating the key aspects of energy management, communication protocols and future applications of IoT for information systems.

A. Energy Management in IoT

To achieve the maximum utilization of available energy in the application area of tracking mobile targets under IoT implementations for dense sensors deployments areas such as battlefields, L. Xiao et al [38] presented a novel node selection approach based on Knowledge-aware Proactive Nodes Selection (KPNS) scheme. The KPNS scheme is designed to adjust the available proactive nodes according to the prediction accuracy of mobile targets. The KPNS scheme achieves balanced energy consumption by using available leftover energies of the nodes in different areas. The simulations results show the improvement in energy efficiency and decrease in target tracking delays as compared to other Probability-based target Prediction and Sleep Scheduling strategy (PPSS) schemes.

The implementation of IoT in buildings and infrastructures has a key importance in maintaining and managing energy-related issues. F. Terroso-Saenz et al [39] proposed an IoT based holistic solution to analyze large and diverse energy-related data in these infrastructures. The suggested IoT Energy Platform (IOTEP) manages the sensors at the physical level by providing deployment and installation guide. To achieve real-time data gathering a data management level is defined considering heterogeneous in the data. The proposed provides key information from sensors to finalize strategies to manage energy-related issues in buildings. The IoTEP platform is implemented and test on real use case consists of three buildings having hundreds of sensors.

D.T Huynh et al [40] focused the energy consumption during the disseminating of multimedia contents in D2D communication. The authors exploit the Genetic algorithm to manage the energy consumption and resource allocation. Due to the consumption of a considerable amount of energy the algorithm performs multiple steps on the multimedia contents by applying layered multiple description coding. The results achieved seem comprehensive and proposed framework enhanced the disseminating of multimedia content through D2D.

The IoT plays an important role in data acquisition (DAQ) based services in dense sensors deployments. During the data gathering phase from these large number of sensors, the energy management among these sensors is a key factor to gain consistency in data acquisition. H.Ko et al [41] proposed an energy efficient sleep scheduling algorithm (CG-E2S2) to gain data acquisition consistency. By using the Markov decision process (MDP) an optimal sleep duration time of IoT devices is calculated for each sensor node, which enables IoT gateway (GW) for forwarding enhanced data traffic volume and improved data acquisition consistency. The proposed scheme provides a guideline for designing energy efficient IoT environments.

B. Routing Strategies for IoT

D. Chemodanov et al [42] focused on the implementation of geographic routing approaches for IoT based incident-supporting application in edge computing. The authors presented the idea of artificial intelligence aided routing protocol based on the area knowledge from the satellite imaging and applying deep learning for the IoT devices. The research work provided an in-depth study of the repulsive model and repulsive forwarding. A stateless greedy forwarding scheme has been employed to avoid the local minimum problem. The simulation and theoretical results validate the effectiveness of the proposed scheme.

By using the characteristics of sensors the concept of IoT is implemented for the disaster management. Due to the large-scale implementation of sensors the data gathering in a disaster situation is a key issue. F. Al-Turjman [43] proposed a cognitive data delivery approach to address the challenges of data delivery in networks under disaster situations. The suggested cognitive routing protocol consider the key parameters of network remaining energy levels and hop count for path selection in these networks.

R. Morabito et al [44] focused on the implementation of IoT in Multi-access Edge Computing (MEC). The authors suggested an architecture named as Lightweight Edge Gateway for the Internet of Things (LEGIoT) to overcome the issues of low computational capabilities at edge gateway. The architecture is based on the characteristics of microservices and flexibility of lightweight visualizations. The implementation of LEGIoT in real sensor network shows optimized resource management with energy efficiency in different IoT services.

C. Securing Techniques for IoT

To overcome the security issues of IoT, F.A.texixeira et al [45] focused the security aspects of distributed IoT programs and suggested a technique to protect IoT against Buffer Overflow (BOF) attacks. The novel technique considers inter-program links which help to build an inter-program view based on this knowledge correct modelling of the semantics of distributed systems is performed. The algorithm is applied on five ContikiOS applications and achieved better results against buffer overflow attacks as compared to traditional buffer overflow static analysis tools.

To achieve the reliability and confidentiality in distributed data storage systems under IoT implementations, N.chervyakov et al [46] presented an idea of using Redundant Residue Number System (RRNS) with enhanced error correction codes and assigning the value of rank of a number (AR). The suggested

AR-RRNS method provides support in error detection, correction with improved data integrity.

With the growth of IoT, it is required to identify and address the various security issues of IoT. There is a need to define mechanisms to authenticate IoT devices. M.A. Jan et al [47] proposed a payload-based mutual handshaking authentication system for IoT under client-server implementations. The new mutual authentication scheme is based on Constrained Application Protocol (CoAP) which is lightweight and plays a critical role for secure data communication between IoT applications. The proposed scheme is evaluated on a real-world scenario and provides active defense against key security issues such as Denial-of-Service and resource exhaustion with computational efficiency with less overhead.

D. Cloud based IoT Application

The quality of data collected in the cloud of IoT is a key issue. R. Hayat et al [48]presented a Game based approach to enhance the Data-as-Service (DaaS) Provisioning in IoT applications. The scheme manages the Quality-of-Data levels between DaaS services and data consumers having a Q-learning algorithm which enables an agreement between the two negotiating parties. By using Shannon's entropy Multi Attributes Decision Making (MADM) algorithm is used for best signal selection during incomplete negotiation information.

H.W.da Silva et al [49] presented the multimedia data delivery strategy in SDN cloud. To overcome the issues of latency-critical IoT applications a novel control plan optimization is suggested using a Cross-Layer SDN Session Control (CLASSICO) architecture. The approach achieves QoS/QoE in IoT applications under SDN cloud environments for multimedia content delivery.

IV. Conclusion

The ongoing era of the Internet of Thing will revolutionize the technological world. The key issues during IoT implementation are focused and highlighted by different research communities. The aim of this Special Section is to solicit the efforts and ongoing research work in the domain of resource management in IoT. This issue has elaborated the key aspects of energy management, communication protocols and future applications of IoT for information systems. The important aspects of energy management, the role of routing protocol and security management in IoT are focused by the researchers. This issue has provided an opportunity for the research community across the globe to share their ideas on this newly emerging field of IoT.

V. Acknowledgment

We would like to sincerely thank all the authors and reviewers for the tremendous efforts towards the success of this special issue. We would also like to thank to the Editor-in-Chief Prof. Peter Sloot.

References

[1] S. Li, L. Da Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[3] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of thingsŮa survey of topics and trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[4] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431 – 440, 2015. [Online]. Available: //www.sciencedirect.com/science/article/pii/S0007681315000373

[5] M. Nitti, V. Pilloni, G. Colistra, and L. Atzori, "The virtual object as a major element of the internet of things: a survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1228–1240, 2016.

[6] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: Vision and challenges," *Ad Hoc Networks*, vol. 33, pp. 87–111, 2015.

[7] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454, 2014.

[8] A. Meddeb, "Internet of things standards: who stands out from the crowd?" *IEEE Communications Magazine*, vol. 54, no. 7, pp. 40–47, 2016.

[9] V. Gazis, "A survey of standards for machine to machine (m2m) and the internet of things (iot)," *IEEE Communications Surveys & Tutorials*, 2016.

[10] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and M. Z. Sheng, "Iot middleware: A survey on issues and enabling technologies," *IEEE Internet of Things Journal*, 2016.

[11] C. Pham, Y. Lim, and Y. Tan, "Management architecture for heterogeneous iot devices in home network," in *Consumer Electronics, 2016 IEEE 5th Global Conference on*. IEEE, 2016, pp. 1–5.

[12] H.-C. Hsieh, K.-D. Chang, L.-F. Wang, J.-L. Chen, and H.-C. Chao, "Scriptiot: A script framework for and internet-of-things applications," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 628–636, 2016.

[13] F. Samie, L. Bauer, and J. Henkel, "Iot technologies for embedded computing: A survey," in *Hardware/Software Codesign and System Synthesis (CODES+ ISSS), 2016 International Conference on*. IEEE, 2016, pp. 1–10.

[14] J. Tan and S. G. Koo, "A survey of technologies in internet of things," in *Distributed Computing in Sensor Systems (DCOSS), 2014 IEEE International Conference on*. IEEE, 2014, pp. 269–274.

[15] P. Ray, "A survey on internet of things architectures," *Journal of King Saud University-Computer and Information Sciences*, 2016.

[16] V. Gazis, M. Görtz, M. Huber, A. Leonardi, K. Mathioudakis, A. Wiesmaier, F. Zeiger, and E. Vasilomanolakis, "A survey of technologies for the internet of things," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International*. IEEE, 2015, pp. 1090–1095.

[17] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

[18] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[19] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[20] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[21] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and zigbee standards," *Computer communications*, vol. 30, no. 7, pp. 1655–1695, 2007.

[22] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, 2010.

[23] I. Ishaq, D. Carels, G. K. Teklemariam, J. Hoebeke, F. V. d. Abeele, E. D. Poorter, I. Moerman, and P. Demeester, "Ietf standardization in the field of the internet of things (iot): a survey," *Journal of Sensor and Actuator Networks*, vol. 2, no. 2, pp. 235–287, 2013.

[24] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1389–1406, 2013.

[25] V. Karagiannis, P. Chatzimisios, F. Vazquez-Gallego, and J. Alonso-Zarate, "A survey on application layer protocols for the internet of things," *Transaction on IoT and Cloud Computing*, vol. 3, no. 1, pp. 11–17, 2015.

[26] R. H. Weber, "Internet of things–governance quo vadis?" *Computer Law & Security Review*, vol. 29, no. 4, pp. 341–347, 2013.

[27] R. Dijkman, B. Sprenkels, T. Peeters, and A. Janssen, "Business models for the internet of things," *International Journal of Information Management*, vol. 35, no. 6, pp. 672 – 678, 2015. [Online]. Available: //www.sciencedirect.com/science/article/pii/S0268401215000766

[28] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, "Ethical design in the internet of things," *Science and engineering ethics*, pp. 1–21, 2016.

[29] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, "Access control in the internet of things: Big challenges and new opportunities," *Computer Networks*, vol. 112, pp. 237–262, 2017.

[30] J. Guo, I.-R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1 – 14, 2017. [Online]. Available: //www.sciencedirect.com/science/article/pii/S0140366416304959

[31] M. R. Palattella, M. Dohler, A. Grieco, G. Rizzo, J. Torsner, T. Engel, and L. Ladid, "Internet of things in the 5g era: Enablers, architecture, and business models," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 3, pp. 510–527, 2016.

[32] P. Gaur and M. P. Tahiliani, "Operating systems for iot devices: A critical survey," in *Region 10 Symposium (TENSYMP), 2015 IEEE*. IEEE, 2015, pp. 33–36.

[33] O. Hahm, E. Baccelli, H. Petersen, and N. Tsiftes, "Operating systems for low-end devices in the internet of things: A survey," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 720–734, 2016.

[34] M. H. A. Abdelsamea, M. Zorkany, and N. Abdelkader, "Real time operating systems for the internet of things, vision, architecture and research directions," in *Computer Applications & Research (WSCAR), 2016 World Symposium on*. IEEE, 2016, pp. 72–77.

[35] A.-C. G. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "Towards a software-defined network operating system for the iot," in *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 2015, pp. 579–584.

[36] M. Amjad, M. Sharif, M. K. Afzal, and S. W. Kim, "Tinyos-new trends, comparative views, and supported sensing applications: A review," *IEEE Sensors Journal*, vol. 16, no. 9, pp. 2865–2889, 2016.

[37] F. Javed, M. K. Afzal, M. Sharif, and B.-S. Kim, "Internet of things (iots) operating systems support, networking technologies, applications, and challenges: A comparative review," *IEEE Communications Surveys & Tutorials*, 2018.

[38] X. Liu, S. Zhao, A. Liu, N. Xiong, and A. V. Vasilakos, "Knowledge-aware proactive nodes selection approach for energy management in internet of things," *Future generation computer systems*, 2017.

[39] F. Terroso-Saenz, A. González-Vidal, A. P. Ramallo-González, and A. F. Skarmeta, "An open iot platform for the management and analysis of energy data," *Future Generation Computer Systems*, 2017.

[40] D.-T. Huynh, M. Chen, T.-T. Huynh, and C. H. Hai, "Energy consumption optimization for green device-to-device multimedia communications," *Future Generation Computer Systems*, 2017.

[41] H. Ko, J. Lee, and S. Pack, "Cg-e2s2: Consistency-guaranteed and energy-efficient sleep scheduling algorithm with data aggregation for iot," *Future Generation Computer Systems*, 2017.

[42] D. Chemodanov, F. Esposito, A. Sukhov, P. Calyam, H. Trinh, and Z. Oraibi, "Agra: Ai-augmented geographic routing approach for iot-based incident-supporting applications," *Future Generation Computer Systems*, 2017.

[43] F. Al-Turjman, "Cognitive routing protocol for disaster-inspired internet of things," *Future Generation Computer Systems*, 2017.

[44] R. Morabito, R. Petrolo, V. Loscri, and N. Mitton, "Legiot: a lightweight edge gateway for the internet of things," *Future Generation Computer Systems*, vol. 81, pp. 1–15, 2018.

[45] F. A. Teixeira, F. M. Pereira, H.-C. Wong, J. M. Nogueira, and L. B. Oliveira, "Siot: Securing internet of things through distributed systems analysis," *Future Generation Computer Systems*, 2017.

[46] N. Chervyakov, M. Babenko, A. Tchernykh, N. Kucherov, V. Miranda-López, and J. M. Cortés-Mendoza, "Ar-rrns: Configurable reliable distributed data storage systems for internet of things to ensure security," *Future Generation Computer Systems*, 2017.

[47] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for internet of things," *Future Generation Computer Systems*, 2017.

[48] R. Hayat, E. Sabir, E. Badidi, and M. ElKoutbi, "A signaling game-based approach for data-as-a-service provisioning in iot-cloud," *Future Generation Computer Systems*, 2017.

[49] H. W. da Silva, F. R. Barbalho, and A. V. Neto, "Cross-layer multiuser session control for optimized communications on sdn-based cloud platforms," *Future Generation Computer Systems*, 2017.