Smart World: Convergence of Communication Networks and Enabling Technologies for Ubiquitous Services

Shaftab Ahmed
Department of Software Engineering
Bahria University, Islamabad, Pakistan
Email: Shaftab_2010@yahoo.com

***Abstract* – The development of intelligent hardware and advancements in data communications networks have led to the development of smart technologies with Internet connectivity. Such devices are called Internet of Things (IoT) and are used to integrate intelligent solutions. The Service Oriented Architecture (SOA) has added virtuality, scalability, manageability, seamless cross platform communication and integration for ubiquitous availability. Mobile communication technologies have matured to 4G and 5G levels for global connectivity and use of satellite communications also called Wireless World Wide Web (WWWW). Progress towards 6G and 7G networks will address the difficulties of earlier standards, making space roaming a reality. Convergence of data communication paradigms is imminent due to advances in network technologies and evolving reliance on software defined networks. While the use of cloud computing and virtual storage is rapidly being accepted by computer users, the security of information particularly personal data and healthcare has to be improved. In this paper we review the enabling technologies of Next Generation Networks (NGN) for smart world and migration to IPv6 suit. In addition we discuss broadband access technologies merged with communications and network systems being used by enterprises, shopping complexes, healthcare systems, emergency response systems and traffic control.**

Keywords* - *SDN; wwww; SOA; IoT; BMS; WSN.

I. INTRODUCTION

Data communications and networking have become a life line of modern society. The world is experiencing a vital change due to the availability of smart solutions for all kinds of activities. The computation and data storage are not limited to desktop or central servers; instead the resources may be in virtual domain accessible through intelligent service providers. The services may also include the Quality of Service (QOS) and bandwidth on demand options available for prospective users.

The de-centralization of data storage and computation is the outcome of intelligent terminal equipment development and the use of computer networks. Internet revolutionized the Information Communication Technologies (ICT) activities by providing a gateway to users of all domains to share, communicate or use the data services offered by Internet service providers (ISPs). Service Oriented Architecture (SOA) has revolutionized the ICT activities leading to virtual storage, computation and a variety of service frameworks [1]. Cloud is the term used to describe virtual service paradigms, which use virtualized infrastructures to offer Software as a Service (SaaS) and Platform as a Service (PaaS) over Infrastructure as a Service (IaaS) allowing users to share physical resources in multitenant applications [2]. Network as a Service (NaaS) enables the use of heterogeneous hardware and software communication between devices and computers for exchange of information [3]. Software Defined Network (SDN) divides a computer network into Control Plane and Data Plane for better management and controllability through software.

Today we experience a convergence of technologies where smart phones, wireless sensors, laptops, tablets etc. are able to easily use the storage / computation services in virtual domain easily. The users of these Information Technology (IT) resources may not be professional computer scientists or engineers. The Internet of Things (IoT) architecture supports embedded sensors like Radio Frequency Identification (RFID) tags / reader, near field sensors (NFS), near field communication (NFC) and actuators [4]. The enormous amount of data from these devices has to be rationalized, processed, stored and presented in an easy to interpret form. Various solutions are available for this purpose however, custom tailored versions are preferred.

The mobile communication standards have evolved from 1G to 4G and now progressing towards 5G to 7G. The first generation (1G) was developed using analog systems available on Public Switched Telephone Networks (PSTN) and had a data rate of 2.4Kb/Sec. The second generation (2G) used digital data communication networks and technologies. The third generation (3G) is the outcome of success of 2G and is designed for user-user communication. It also laid down specifications of a framework for future growth of mobile communication technologies. The framework supports three tiers, i.e. Access technologies, Transport technologies and User applications [5]. The fourth generation (4G) was developed to integrate the cellular network technologies with Wi-Fi and fixed network technologies. The fifth generation (5G) increased flexibility in global communication systems to include satellite communications, hence, the evolution of wireless worldwide web (wwww) technologies [6]. The sixth generation (6G) is developed to overcome the problems of 5G, i.e. technology and standard variations in global communications systems [7]. The seventh generation (7G) will support space roaming through global integration of mobile communications with no data capacity and mobility restriction across countries and continents seamlessly [8].

Broadband access technologies, integrated with mobile communication platforms, will enhance the scope of distributed processing applications available for effortless usage through mobile applications [9]. Mobile application development is the fastest growing field in IT. Mostly Java programming language is used for application development

ISBN: 978-1-61208-679-8

and Java Virtual Machine (JVM) supports cross platform portability. The rest of the paper is organized as follows: in Section II we present relevant research work for IoT infrastructure development. In Section III, we discuss software and data network communication technologies in the context of smart world architectures. In Section IV, we present the challenges posed by IoT culture and the need to develop elaborate security mechanisms with forensic data management leading to enhanced and trustful usage of IoT devices. In addition we discuss future directions in security enhancements for IoT expansion in the context of distributed computing and data management involving Internet of things through hierarchical security policies.

II. RELATED WORK

Ubiquitous connectivity using Wi-Fi, Wi-Max and other similar technologies have supported the development of smart solutions for home / office automation, healthcare, guidance / surveillance systems, etc. Wireless sensors and actuators have led to the development of intelligent devices enabled to communicate over the web called IoT. The IT developers provide plug and play environments to integrate hardware and software for IoT. Hence, data acquisition, storage and sharing are effortless [10]. From a larger perspective, applications may collect measure and use the information for expert systems or Decision Support Systems (DSS). Convergence of technologies and the interests of IT developers, business communities and virtualization of multitenant, multiplatform architectures have extended the scope of service providers and IoT solution providers [11].

Social networking has become a means of evolving close knit communities. The registration, discovery and session management features allow interaction and usage of common resources through virtual networks abstracted through layered architecture. Ubiquitous services are available through hand held smart devices, which use wireless and fixed networks and communication systems in virtual domain. Distributed information systems are available to the users through converged IT solutions.

Healthcare support by intelligent data acquisition and management system has helped patients and doctors to avail all time connectivity, consultation and emergency response [29]. Home care systems have evolved where data periodically collected through sensors is measured, aggregated and sent to the servers / nursing stations where it is processed and saved in the personal history of the patients. Intelligent agents analyze the clinical data to monitor patients' progress and raise suitable alerts whenever required, under appropriate protocols and policies [36]. Alerts may be related to medicine intake, laboratory tests, exercise schedule, nutrition and procedures for treatment prescribed by the physician. In some cases, the alerts may be raised for imminent medical emergency, like heart attack or stroke, while the patient is unaware of the symptoms [37].

The growth of IoT and its integration in smart systems has increased vulnerability of digital systems. In prevailing security mechanisms, authentication, authorization and access control is extended to distributed data networks and eventually the cloud architectures. These systems have been developed as a result of research carried out in the last few decades to provide reasonably effective solutions in ICT industry. Data management in heterogeneous distributed systems accessible through smart systems with embedded IoT demand inclusion of new features for forensic studies.

Inclusion of intelligent devices capable to communicate with digital systems autonomously may cause serious security problems. Hence, new features like registration, verification and forensic data management are required for IoT in highly virtualized distributed systems in smart networks at home, neighborhood, city systems and the world at large. A home device authentication method based on Public Key Infrastructure (PKI) has been discussed in [12]. Light weight PKI has been proposed for mobile and hand held devices used in smart systems [13]. A model forensics aware system design for IoT in future systems has been presented by [14]. The concept of Certification Authority (CA) to maintain forensic information record about manufacturer code, unit number, seller / buyer / current owner identity along with password history, session key management trail with reasonable depth can be useful to make IoT security practical. Security information may be managed through hierarchical levels for quicker services and fault tolerance. The IoT may be linked to mobile, wireless and wired network networks with a possibility to extract trail of events for forensic study.

III. CONVERGENCE OF TECHNOLOGIES

Availability of broadband connectivity and multimedia support at affordable prices has merged data communications and computer networks. Developments of Wireless Sensor Networks (WSN) smart phones, hand held devices and intelligent host system developments have transformed the world into a digital society. IT applications range from home automation, healthcare, and education to industrial automation, environmental applications, e-government and smart city solutions. Increasing use of digital contents in data transmission over IP based networks has converged technologies in enterprises, homes and industry [10]. Virtuality is the popular way to integrate software, hardware and support systems into service oriented architecture (SOA). Out of these developments, a rapidly growing market of smart solutions has emerged [16].

Virtualization of computer hardware, software and services has led to integration of IT and Communication Technology (CT) for smart solutions. Wireless Internet aware intelligent technologies are rapidly becoming acceptable in human communities for various purposes. The evolving scenarios will allow integration of solutions by using interoperable IoT devices and Software Defined Networking (SDN). Figure 1 shows Next Generation Network (NGN) architecture based on layered model to integrate Original Equipment Manufacturers (OEMs), network technology developers, Telecommunication service providers, Radio / television and Internet Service Providers (ISP).

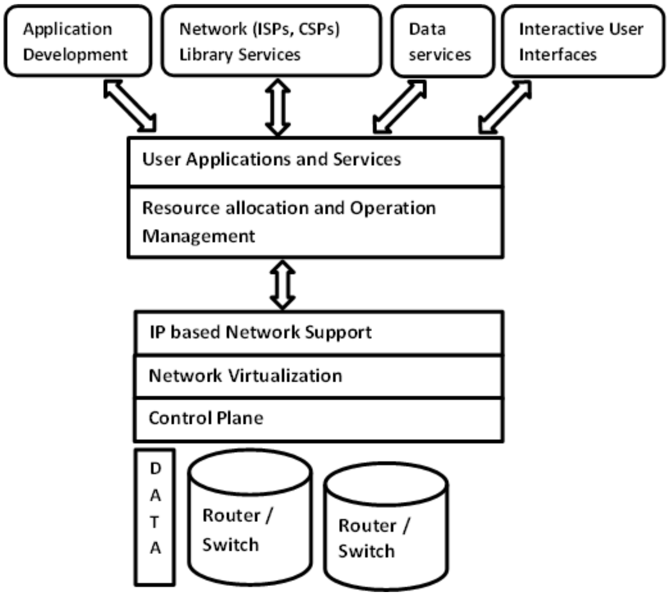
Application Development
Network (ISPs, CSPs) Library Services
Data services
Interactive User Interfaces
User Applications and Services
Resource allocation and Operation Management
IP based Network Support
Network Virtualization
Control Plane
D A T A
Router / Switch
Router / Switch

Figure 1. Convergence of network technolgies and the layered architecture over Software Defined Network (SDN)

Telecommunication companies and Radio/ Television are increasing use of Internet service model for all time and anywhere availability. Similarly the Packet switching, circuits switched to broad cast networks are offered through a common service layer, which uses protocol conversions, policy, Service Level Agreement (SLA). Converged networks require elaborate security, privacy and accountability policies for borderless communication [15].

Convergence of wireless, optical fiber and land based digital communication technologies with computer technologies for computation; data management and presentation etc. have ignited innovative growth of smart devices and applications in everyday life. The smart cities, smart enterprises / buildings, disaster management, medical / eHealthcare, smart grids and road traffic are the realms of the smart world [16][17]. We discuss the enabling technologies, network communication protocols and the security issues stemming out as a result of private and personal engagement through social networking [18][19].

A. Technical perspective

Smart data communication technologies have promoted easy integration of hardware and customized software solutions for distributed systems. The middleware support vendor neutral, platform independent hardware / software interface required to meet standards of interoperability, portability, transparency, mobility etc. We discuss example of smart city supporting eHealthcare, building management, road traffic and smart grids as under:

i. Smart City Management Systems (SCMS)

The smart solutions for everyday life as well as professional and industrial systems have given birth to the concept of “smart city”. It is implemented through layered architecture where physical spaces, buildings, enterprises, transport utilities etc., are abstracted into city systems layer through ICT infrastructure [20]. These systems provide access to latest information concerning the city through Internet to be used for analysis and decision support systems. SOA has helped in making city systems ubiquitous and pervasive [21][22]. Convergence of networks plays a key role in seamless access to resources irrespective of software, hardware, and service platform. Network services play a key role by hiding platform and network layers in allowing access to resources.

ii. Building Management Systems (BMS)

Most of the enterprise buildings today have computer networks, which support services like database / document management, ecommerce, paging, video coverage along with Internet access. Intelligent building management systems are supported by IoT devices for autonomous data collection and submission to server; they may share data with other IoT devices in the neighborhood [23][24]. Electric power management of illumination lights, room air-conditioning and other activities can be handled by smart devices in coordination with server under a policy [25]. Ubiquitous cloud services may be used to provide anywhere, anytime availability of information. Smart city projects can be extended to integrate features offered by building management systems for various purposes like security and remote monitoring / management. A cyber-home connected to a service provider over the Cloud architecture is shown in Figure 2.

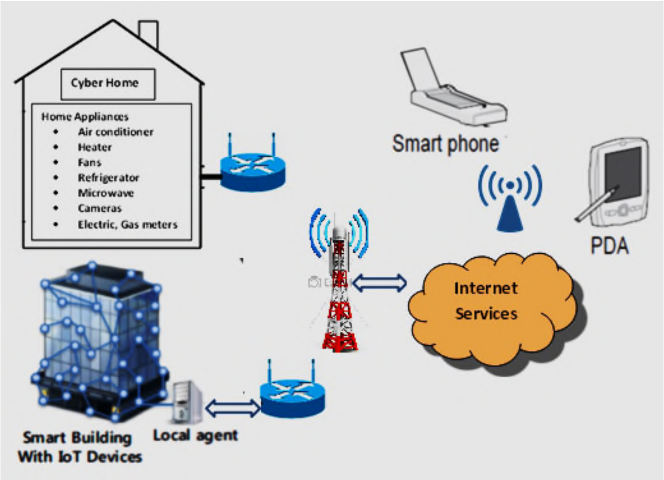

Figure 2. IOT: Smart Buildings and home architecture [Internet clipart resources]

Information sharing requires security features to be implemented in a building management system to avoid malicious activities. The IoT device authentication at home or office can be implemented by a hierarchical PKI based stack where the

Certification Authority (CA) at various levels plays a key role [25-28].

iii. Medical and Healthcare Systems (MHS)

Home care and e-Healthcare models are being rapidly developed to provide better quality of life, protection and health monitoring services. The aged or disabled people, patients getting prolonged medical treatment or requiring post-surgical monitoring are the clients for smart homes and smart cities. User friendly Decision Support Systems (DSS) over the cloud architecture allow the doctors to interactively make medical therapy schedule while getting patient's inputs on line if required [29]. Doctor's prescription for clinical tests, reports and patient monitoring may be managed online [30]. The IT and clinical tools are used for data searching and presentation to patients, doctors, pharmacists and researchers. Proactive monitoring of lab reports and the record of exercise / physiotherapy schedules is done by intelligent agents embedded in these systems. Figure 3 shows a typical e-Heathcare system using IoT devices.

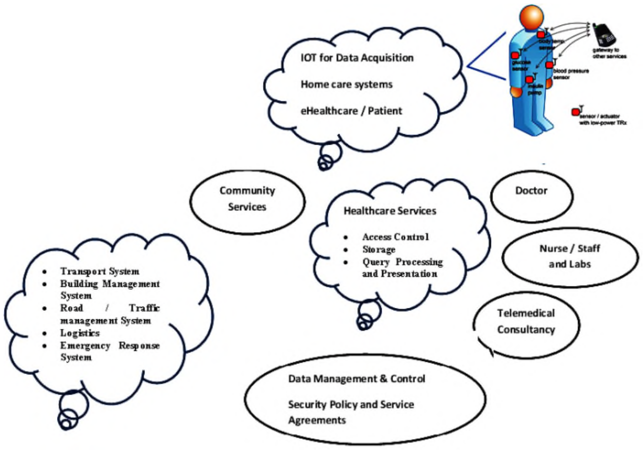
IOT for Data Acquisition
Home care systems
eHealthcare / Patient
gateway to other services
blood pressure sensor
sensor / actuator with low-power TRx
Community Services
Healthcare Services
Access Control
Storage
Query Processing and Presentation
Doctor
Nurse / Staff and Labs
Telemedical Consultancy
Transport System
Building Management System
Road / Traffic management System
Logistics
Emergency Response System
Data Management & Control
Security Policy and Service Agreements

Figure 3. An e-Healthcare system using IoT devices

iv. Intelligent transport systems (ITS)

The industrial developments and availability of opportunities for technical financial and social growth has led to concentration of human population in big cities. Transport management in such cities is quite complex on account of varying traffic conditions, road accidents, etc. Conventional traffic control is supported by intelligent transport systems by using statistical record and live information for traffic forecast and raising alerts. The information is presented for traffic management and driving support through telecommunication system. The drivers can get traffic information on line while in transit or at home through intelligent devices and alerts. The emergency support systems along with multimedia services may be of great value for the commuters in many situations. Besides access to network services they may be able to communicate with other vehicles on the road. The fiber cables laid alongside long haul highways provide high speed data access through access points for wireless communication. Intelligent transport system consists of navigation, electronic toll collection, driving safety etc. [31][32]

B. Enabling technologies for convergence

Network hardware and software systems use technologies, which support interoperability and easy configurability through software. Object oriented programming tools are extensively used for this purpose. JAVA supports better portability across hardware and software platforms by using Java Virtual Machine (JVM) at an intermediate layer. It has won wide acceptability particularly for hand held smart devices using embedded operating systems like IOS, Tiny Linux, Android etc. Enabling technologies for convergence of IT activities are discussed as under:

i. Smart devices and IoT culture

Internet has been widely accepted norm of the modern world making it a global village engulfed into a virtual reality. The IoT culture and use of smart devices over available network solutions will add new dimensions to the social systems covering all areas of social, cultural and technical activities [33]. Wireless sensor networks often use low power, maintenance free devices at the front end and Wi-Fi, Wi-Max or land based communication systems for data network. IoT devices use wireless sensors for autonomous data collection, decision making and reporting events to servers under a policy.

ii. Social Networking

The participation of humans of all ages, professions and interests has given rise to formation of cyber communities spanning over computer networks. Community is a group of users sharing common interest for example content creators, users, developers and service providers, etc. form a group [34]. Hence, a community in the ICT domain may be seen as interlinked web pages in the Internet cloud. These communities are usually able to interact with each other hence, making bigger picture of social networking. Social networks like LinkedIn, Facebook, Twitter, WhatsApp, etc. have assumed importance for sharing information in professional and social groups or communities. Whereas it is an interesting phenomenon, it is often complicated and dangerous [35].

iii. Cloud Services Architectures (CSA)

An integrated e-Healthcare solution over cloud services architecture may be developed by utilizing web engineering technologies, coupled with software utilities of Hadoop Distributed File System (HDFS) along with a suitable RDBMS (Relational Database Management System) over high speed data communication infrastructure. The characteristics of ubiquitous healthcare system over a cloud should provide inexpensive, flexible, and reliable fault tolerant services [36][37].

iv. Software Defined Network (SDN)

Smart solutions offered through ubiquitous network connectivity and the evolving new paradigms the Internet of Things, smart cities and e-government demand fundamental changes in the network design techniques [38]. Application developers require intelligent management of networks for cloud services architectures hence, SDN is being used for flexibility, scalability and network management.

C. Secure communication protocols

It is estimated that 20 billion IoT devices will be attached to the Internet through ISPs in the next decade [24]. Extensive use of IoT devices will increase vulnerability due to a wider platform open to hackers and their malicious activities. The large number of devices requires low level identification / verification to conceive reasonable security architecture. Hence, a quick transition to Internet Protocol version 6 (IPv6) will be required to meet the enormous increase in devices, data and the handshake for secure communications [39]. The devices will be connected in a hierarchy of levels to reduce the overhead of protocol data and communication.

IV. CONCLUSIONS AND FUTURE DIRECTIONS

The software design and network architectures have to provide solutions for secure data sharing in multitenant domains. Service oriented computing offered in the cloud architectures use virtualized infrastructures to offer Infrastructure as a Service (IaaS) allowing users to share physical resources in multitenant applications.

Computer forensics can be summarized as the process of identifying, collecting, preserving, analyzing and presenting the computer-related evidence in a manner that is legally acceptable by the court of law. Integrity of information through verifiable procedures allows forensic data to be used for evidence. Forensics Aware IoT (FAIoT) [40][41] suggests three layers i.e. Cloud forensics, Network forensics and Device forensics for this purpose. The model is highly distributed hence, a trusted repository may be used for data collection, analysis and evidence extraction. An evidence collection module will monitor all registered IoT devices and store in the repository. To handle such large repository Hadoop Distributed File System (HDFS) has been proposed.

Internet based central registration of IoT for forensics through hierarchy of certification authorities (CA) can be used for security and verifiability. The typical PKI algorithm with some modifications to reduce overheads can be used for this purpose. The certificate may maintain security vectors for manufacturer, buyer, owner history, password history, GIS location etc. distributed at various levels. Secure session logs after TLS handshake at the Internet level can be maintained for forensic studies

REFERENCES

[1] H. Yoshida, R. Take, H. Kishimoto and Y. Hibi, “ Service Oriented Platform” Fujitsu Sci.Tech. J. Vol 46, no. 4, pp 410-419, October 2010.

[2] R. Guha and D. Al-Dabass, “Impact of Web 2.0 and Cloud Computing Platform on Software Engineering” International symposium on electronic system design” 978-0-7695-4294-2/10, IEEE, DOI 10.1109/ISED.2010.48.

[3] W. Gerhardt, C. Cordero, C. Reberger and T. Dolan, “Mobile Network as a Service A New Solution Architecture for Mobile Network Operators” Cisco Internet Business Solutions Group (IBSG), March 2013.

[4] H. Farhady, H. Lee and A. Nakao “Software-Defined Networking: A survey” 1389-1286/_ 2015 Elsevier B.V. All rights reserved, pp79-95, 2015

[5] J. Kremer, “White Paper Near Field Commmunications” JKCS Consulting Services.

[6] M. Farooq, M. I. Ahmed and U. Mohammad, “Future Generations of Mobile Communication Networks” Academy of Contemporary Research Journal V II (I), 24-30, ISSN: 2305-865X, Resource Mentors (Pvt) ltd, 2013.

[7] J. Sen, “ Convergence & Next Generation networks” Whitle paper, Tata Consultancy Services Ltd., Global ICT standardization forum for india (GISFI), Jul 2009

[8] J. Alleman and P. Rappoport, “The unsustainability of access competition ITU”, The Future of Communications in Next Generation Networks, 15-16 January 2007.

[9] X. Li, A. Gani, R. Salleh and O. Zakaria, “The Future ofMobile Wireless Communication Networks” 978-0-7695—3522-7,IEEE Computer Society, DOI 10. 1109／ICCSN. 2009. 105.

[10] R. C. Huacarpuma et al,“ Distributed Data Service for Data Management in Internet of Things Middleware” Sensors 2017, 17, 977; doi:10.3390/s1705097 .

[11] J. Lopeza, R. Riosa, F. Baob and G. Wang, “Evolving Privacy: From Sensors to the Internet of Things, Journal of Future Generation Computer Systems May 29, 2017.

[12] D. Lee, J. Han and Y. Lee, "Home Device Authentication Method Based on PKI", , vol. 02, no. , pp. 7-11, 2007, doi:10.1109/FGCN.2007.143

[13] H. Jin and H. Chen, “Lightweight Session key Management scheme in Sensor Networks” FGCN '07 Proceedings of the Future Generation Communication and Networking - Volume 02 pp 3-6, ISBN:0-7695-3048-6, doi>10.1109/FGCN.2007.159.

[14] Shalini, V. N. Singh, M. Yadav and P. Rastogi, “Forensic Approach for Data Acquisition of Smart Phones to Meet the Challenges of Law Enforcement Perspective” J Indian Acad Forensic Med. April-June 2015, Vol. 37, No. 2 ISSN 0971-0973A.

[15] M. T. Abdullah, R. Mahmod , A. A. Ghani, M. Z. Abdullah, and A.Bakar, “Advances in Computer Forensics” IJCSNS International Journal of Computer Science and Network Security”, VOL.8 No.2, February 2008.

[16] M. Al-Hader and A. Rodzi,” The smart City Infrastructure Development & Monitoring” Theoratical and Empirical Researches” number 2(11) / May 2009.

[17] Z. Alazawi, O. Alani, M. Abdljabar, S. Altowaijri and R. Mehmood, “ A Smart Disaster Management System for Future Cities”, WiMobCity’14, August 11, 2014, Philadelphia,USA. doi.org/10.1145/2633661.2633670.

[18] C. Cerrudo, “An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks” a white paper, IOActive, Inc., 2015.

[19] “Cyber Physical Systems – Situation Analysis” NIST: National Institute ofstandards and Technology, March 2012.

[20] L. Anthopoulos, “From Digital to Ubiquitous Cities: Defining a Common Architecture for Urban Development” IEEE Computer Society, ISBN: 978-0-7695-4149-5 doi>10.1109/IE.2010.61.

[21] T. Na and T. mA. Pardo, “Conceptualizing Smart City with Dimensions of Technology, People, and Institutions” Proceedings of the 12th Annual International Conference on Digital Government Research, Dg.o’11, ACM 978-1-4503-0762-8/11/06.

[22] J. Lee, S. Baik, and C. Lee, “Building an Integrated Service Management Platform for Ubiquitous Ecological Cities”, Computer, vol. 44, no. , pp 56-63, June 2011, doi:10.1109/MC.2011.131.

[23] M. Batty et al, “smart Cities of the future” Eur. Phys. J. Special Topics 214, 481–518 (2012), doi: 10.1140/epjst/e2012-01703-3.

[24] J. Yu, M. Kim, H. Bang and S. Kim, “IoT as a applications: cloud-based building management systems for the internet of things” Multimedia Tools and Applications • July 2015 doi 10.1007/S11042-015-2785-0.

[25] L. Ngo, "Service-oriented architecture for home networks”, TKK T-110.5190 Seminar on Internetworking 2007-3-4/5 Helsinki University of Technology, Finland.

[26] G. Meyer and A. Stander, “Cloud Computing:The Digital Forensics Challenge” Proceedings of Informing Science & IT Education Conference 2015, pp 285-299.

[27] L. Vrizlynn and L. Thing, “ Cyber Security for A Smart Nation” ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7238277.

[28] D. Lillis, B. A. Becker, T. O’Sullivan and M. Scanlon, “ Current Challenges and Future Research Areas for Digital Forensic Investigation” The 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016), Florida, USA, May 2016, arXiv:1604.03850v1 [cs.CR].

[29] M. Hassanalieragh et al, “Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-basedProcessing: Opportunities and Challenges” IEEE International Conference on Services Computing, 978-1-4673-7281-7/15, DOI 10.1109/SCC.2015.47, 2015.

[30] S. S. Ponedal and M.Tucker,”UnderstandingDecision Support Systems” journal of managed care pharmacy jmcp 2002 vol. 8, no. 2.

[31] S. L. Suen, S. Henderson,”Aapplication of Intelligent Transportation Systems to Enhance Vehicle Safety for elderly and Less able travellers” 16th International Technical Conference on the Enhanced Safety of Vehicles , The National Academies of Sciences, Engineering, and Medicine, DOTHS808759 Volume: 1 pp. 386-94.

[32] J. Walker, “Intelligent Transportation Systems Report for Mobile, GSMA Connected Living Programme,GSM Association, 2015.

[33] P.C.Jain and K.P.Vijaygopalan, “ RFID and Wireless Sensor Networks” Proceedings of ASCNT – 2010, CDAC, Noida, India, pp. 1 – 11.

[34] A. Elmagarmid, A. Samuel and M. Ouzzani, “Community Cyber Infrastructure Enabled Discovery in Science and Engineering” Computing in Science and Engineering 10(5):46 - 53 • October 2008.

[35] K. Malagi, A. Angadi and K. Gull, “Survey on Security Issues and Concerns to Social Networks” International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[36] C. Orwat, A. Graefe and T. Faulwasser, “Towards pervasive computing in health care – A literature review” BMC Medical Informatics and Decision Making 2008, 8:26 doi:10.1186/1472-6947-8-26.

[37] E. Sazonov, K. Janoyan and R. Jhac, “Wireless Intelligent Sensor Network for Autonomous Structural Health Monitoring, doi=10.1.1.99.4283

[38] “SDN and the Future of Service Provider Networks” Fujitsu Network Communications Inc., 2013.

[39] Jara1, L. Ladid and A. Skarmeta, “The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities” Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 4, number: 3, pp. 97-118.

[40] D. Loomis and B. Wohnsiedler, “ The ‘Internet of Things’ (IoT)– Opportunities and Risks” American Society of Safety Engineers , ASSE-15-744, Professional Development Conference and Exposition, 7-10 June, 2015.

[41] S. Zawoad and R. Hasan, “FAIoT : Towards Building a Forensics Aware Eco System for the Internet of Things” 12th IEEE International Conference on Services Computing (SCC), DOI: 10.1109/SCC.2015.46.