ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

A Case study on Smart City Challenges, Technological Factors and Security Analysis

K.Harikrishnan[1], K.Balamurugan[2]

Assistant Professor, Electrical & Electronics Engineering, Sri Ramakrishna Engineering College, Coimbatore, India [1]
Assistant Professor, Electrical & Electronics Engineering, Sri Ramakrishna Engineering College, Coimbatore, India [2]

***Abstract*— Smart cities have attracted an in depth and increasing interest from science and industry throughout the world. The smart city is developed, deployed and maintained with the help of Internet of Things (IoT), therefore becoming smarter than before. India has recently developing and constructing Smart Cities to fulfill the demands of growing and urbanizing population. Smart City includes renovation of existing cities as rural population shifts into urban areas. The objective is to handle some of the customized services in a Smart City environment and also concentrates on the challenges as well as the key areas for development in India. The existing practices, challenges and security analysis with respect to their performance are discussed.**

***Index Terms*—Internet of Things, Security Analysis, Smart City, Urbanization.**

I. INTRODUCTION

Due to the rising of the population density in urban cities, infrastructure and services are needed to address the requirements of the residents. There is a significant increase for digital devices base on the requirement of residents e.g. sensors, actuators, and smartphones that drive to very large business potentials for the IoT, since all devices could interconnect and communicate with each other on the Internet. [1] The next revolution of the Internet will make it possible to provide suitable interconnections among the objects. The interconnection among the various objects based on the IoT is shown in figure 1.

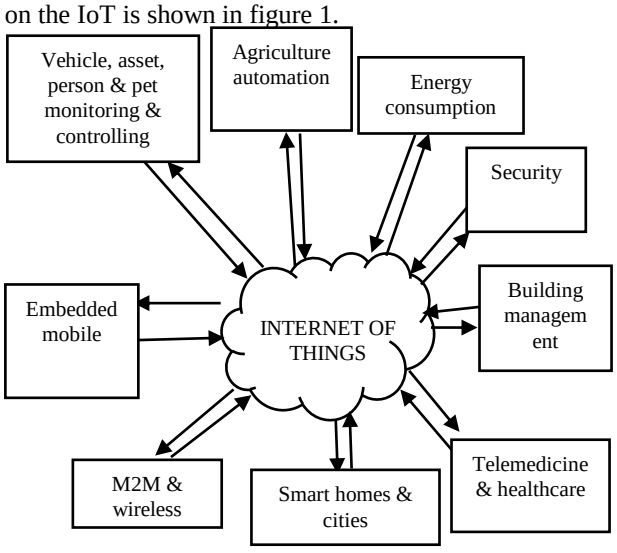

Fig. 1. Interconnection of IoT

Smart Cities are the integration of information technology, telecommunications, urban planning, smart infrastructure and operations in an environment geared to maximize the quality of life for a city's population. Cities are built on the three pillars of Infrastructure, Operations and People. For instance, a Smart City's power distribution infrastructure will be based on Smart Grid technologies, which will integrate with local power demand patterns, grid supply variations, and a well-defined operational process – to manage the available energy most efficiently. The smart cities perform well in six dimensions as shown in table 1.

TABLE I: DIMENSIONS AND EXPECTATIONS FOR SMART CITY

S.No	Dimensions	Expectation for Smart city
1.	Smart Governance	Political strategies and perspective, Participation in decision making
2.	Smart People	Participation in public life and creativity
3.	Smart Living	Health and Safety issues, Housing facilities
4.	Smart Environment	Environment pollution monitoring and control, resource management
5.	Smart Mobility	Strong Transport System and ICT infrastructure
6.	Smart Economy	Entrepreneurship, Production of Goods

II. TECHNOLOGIES IN SMART CITIES

The IoT is a broadband network that uses standard communication protocols while its convergence point is the Internet. The main thought of the IoT is that the universal presence of objects which will be measured, inferred, understood which will amendment the atmosphere. It involves in addition to sophisticated technologies of computer and communication network outside, still including many new supporting technologies of Internet of Things, such as collecting Information Technology, Remote Communication Technology, Remote Information Transmission Technology, Sea Measures Information Intelligence Analyzes and Controlling Technology.

A. Radio-Frequency Identification (RFID)

The technology is classified into three categories based on the method of power supply provision in Tags: Active RFID, Passive RFID and Semi Passive RFID. The main components of RFID are tag, reader, antenna, access controller, software and server. It is more reliable, efficient, secured, inexpensive and accurate. These systems consisting of readers and tags are playing a key role in the

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

context of the IoT. By applying these technologies to any involved object, it is possible to carry out their automatic identification and assign a unique digital identity to each object, in order to be incorporated in the network and related to the digital information and service [2].

B. Near Filed Communication (NFC)

Near Field Communication (NFC) is a set of short-range wireless technology, typically requiring a distance of 4 cm. Through NFC it is simpler to make transactions, exchange digital content, and connect electronic devices based on touch. Other smart functions of the NFC include enabling the users to do the following through their mobile devices: using electronic coupons; receiving texts, pictures and videos of products and services by scanning street or mall posters; point-point money transfers from one mobile device user to another by entering PIN number, which marks breakthrough from traditional mode of electronic money transfer.

C. Beacon

BLE beacons is a low power wireless data transfer device which continually relay a discovery signal that is received by BLE enabled smartphones within the range of transmission. The communication range of a beacon is 70 meters. Most smartphones today support BLE, although it is required that the user has turned on the Bluetooth on his phone, in order to receive the signals from a beacon.

D. Wireless Fidelity

Wireless Fidelity (Wi-Fi) is a technology device which allows other devices to communicate over a wireless signal. WSN based on IoT are used in various applications such as military, homeland security, healthcare, precision agriculture monitoring, manufacturing, habitat monitoring, forest fire and flood detection and so on. [20] WLAN product support any of the IEEE 802.11 together with dual-band, 802.11a, 802.11b, 802.11g and 802.11n.

E. Artificial Intelligence (AI)

Artificial Intelligence refers to electronic environments that are sensitive and responsive to the presence of people. In an ambient intelligence world, devices work in concert to support people in carrying out their everyday life activities in easy, natural way using Information and Intelligence that is hidden in the network connected devices [10].

F. ZigBee

ZigBee is one of the protocols developed for enhancing the features of wireless sensor networks. ZigBee technology is created by the ZigBee Alliance which is founded in the year 2001. Characteristics of ZigBee are low cost, low data rate, relatively short transmission range, scalability, reliability, flexible protocol design. It is a low power wireless network protocol based on the IEEE 802.15.4 standard [19]. ZigBee has range of around 100 meters and a bandwidth of 250 kbps and the topologies that it works are star, cluster tree and mesh. It is widely used in home automation, digital agriculture, industrial controls, medical monitoring &power systems.

III. SMART CITY APPLICATIONS

The IoT utilizes the Internet to incorporate heterogeneous devices with each other. In this regard and in order to facilitate the accessibility, all available devices should be connected to the Internet. In order to achieve this target, sensors can be developed at different locations for collecting and analyzing data to improve the usage.

A. Smart Homes

IoT platform in the home enables the automation of common activities. In fact, by transforming objects into information appliances that are connected to each other by using the Internet may perform services via the web interfaces. A large number of smart-home applications use sensor networks. Smart homes could be monitored by using the data that are generated by the sensors [11].

B. Smart Energy and Smart Grids

The utilization of the IoT can furnish intelligent management of energy distribution and consumption in heterogeneous circumstances. The IoT nodes have some abilities such as sensing and networking which raise the possibility of optimal scheduling of energy suppliers. This management can also be extended to emergency conditions. One of the most important results of this extension is fault location, isolating and service restoration (FLISR) [24]. The IoT provides an advanced tool which determines the position of the defective parts, separates them, and applies switching task to recover the largest number of healthy part of the affected energy feeder. Implementing these strategies leads to increase the reliability, power quality and profits [25].

C. Smart parking lots

By enabling smart parking, arrival and departure of various vehicles can be tracked for different parking lots distributed in the city [12]. Consequently, the smart parking lots should be designed in a way to consider the number of cars in each zone [13]. Moreover, new

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

parking lots should be established where a higher number of vehicles are available [14]. This bring advantages for both vehicle owners' and merchants' daily lives in a smart city.

D. Vehicular traffic

Vehicular traffic data are one of the most important data sources in a typical smart city in which, by using these data and applying a suitable analysis, citizens and the government will benefit greatly [12]. Citizens could be also able to use the vehicular traffic data to determine the arrival time to a destination.

E. Surveillance systems

In a smart city, security is the most important factor from the citizens' viewpoint. For this purpose, the whole smart city should be continuously monitored. However, analyzing the data and detecting crimes are very challenging.

F. Environmental pollution

A city cannot be considered as a smart one if its citizens are unhealthy. So a smart city should monitor the environmental pollution and deliver information to citizens, especially to those with health care conditions.

IV. CHALLENGES IN SMART CITY

In both developing and developed countries, primary motive behind the smart city application is respond to sustainable development needs of the society. An overview of smart infrastructure solutions with their sustainable development needs are discussed as follows in table 2.

TABLE II: SUSTAINABLE DEVELOPMENT NEEDS AND INFRASTRUCTURE SOLUTIONS

Sustainable need/ Challenge	Smart infrastructure solutions	Description
Energy/Utility Infrastructure	Smart Meters	Metering of power, water and gas that can provide real time measurement of energy consumption
	Smart Grids	Re-engineering electrical systems through applications of smart meters, smart appliances, and renewable energy resources in order to attain better energy efficiency.
Quality Connectivity	High Speed Internet	Fiber to the Home and other emerging connectivity solutions, including public Wi-Fi and mobile broadband
Urban Infrastructure	Smart LED street Lighting	Light sensors and communication devices to allow lights to communicate with other nearby lights and to be controlled at a city level
Transport/ Parking/ Buildings	Smart Building	Array of sensors and technologies that improve safety, security, energy efficiency and usability.
	Electric Vehicles	Cars which operate on electricity / batteries with appropriate infrastructure for charging stations throughout the metropolis
	Smart Parking	Car parks and street parking locations than transmits real-time information to users
	Smart Traffic Lights	Automated sensing and management of traffic
Environmental Performance	Environmental Sensor Network	Continuous data collection about the condition of air, water, soil and related levels of pollutants
Security and Safety	Video Security	Public safety, crowd management and people counting using sensor networks and networked cameras
City management	Smart city operation center	Monitoring and management of a range of government, transport, environmental and emergency services
Health and education services	Remote healthcare and online education	Products and services for remote access to health services and education

V. SECURITY ANALYSIS

When all the data are collected and analyzed in a common IoT platform, the system can be subjected to several attacks (e.g., cross-site scripting, and side-channel). Besides, such a system is exposed to important vulnerabilities. Furthermore, multi-tenancy of this system can also bring out the security issues and cause the leakage of data. Such security issues in smart cities are discussed as shown in figure 2.

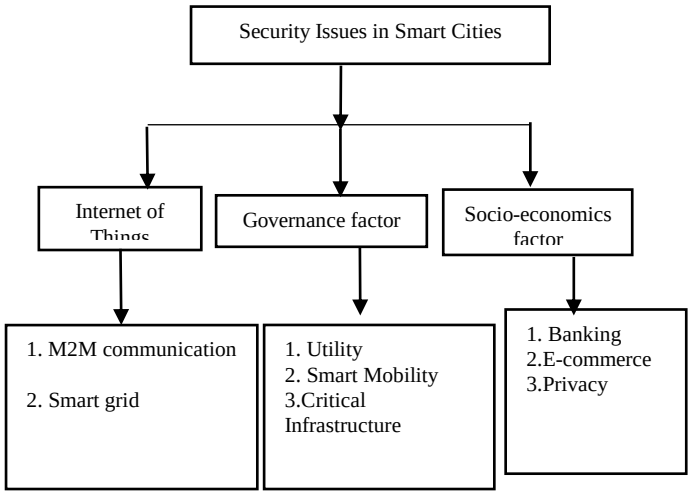

Fig. 2. Security issues in Smart City

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

A. Internet of Things

The Internet of Things (IoT) incorporate a huge number of distinguished and heterogeneous devices, and gives free access to information for various on-line services for smart cities. IoT plays a gigantic role in developing and maintaining the services of a smart city, hence making the issue of secure information flow a huge task with respect to it.

1. M2M Communication

Machine to machine (M2M) communications promise dramatic achievements in the applications and services offered to citizens, making smart city a reality [22]. Machine to machine protocols are used for communication fix the rules of engagement for at least two nodes of a network. Internet Protocol (IP) has become the standard for such communication purposes. Examples of protocols that can be used for communication are: ISA 100A, link Layer, Wireless HART, IPv6 and ZigBee [26]. IPv6 plays a gigantic role in the IoT. According to [27] the main security concerns in M2M communications include:

- Physical Attacks

These attacks include using modified software's for the purpose of fraud. The main breaches that occur due to these attacks are in integrity of data and M2M software's.

- Attacks on authentication tokens

The threats include physical attacks as discussed above and side-channel attacks. The authentication tokens can also be cloned for malicious purposes.

- Configuration Attacks

The example of configuration attacks includes malicious software updates configuration changes that lead to fraud. Moreover, misconfiguration by the user may also occur.

- Protocol Attacks

The protocol attacks are mainly designed against the devices. For example: man-in-the-middle attacks, DoS attacks, and attacks on OAM and its traffic.

- Threats in network security

These attacks mainly target mobile networks. The examples of such threats include impersonation of devices and traffic tunneling between them. Moreover, misconfiguration of the firewall in the devices is also a serious network security breach. The DoS attacks on the network also pose a major problem.

- Breaches in privacy

Privacy is a huge concern of the individuals of a smart city as it is a basic human right. But it becomes very difficult to take care of the privacy of citizens through M2M communications as the ways in which data collection, mining, and provisioning is accomplished are totally different from those that we now know and there are a huge

IEEE Standard Solutions

The solutions available to establish a smart city with respect to security uses IEEE standard solutions for M2M communication. The IEEE provides standard mechanisms for the physical (PHY) and medium access control (MAC) layers which are useful in implementation of a smart city. There exist three families namely IEEE 802.15.4 called as CSMA/CA, IEEE 802.15.1 named as Bluetooth and IEEE 802.15.11 said as Wi-Fi, that can provide low-power and short-range IoT operation for a smart city. The Wi-Fi Protected Access (WPA) is a security protocol that has become the regulation for providing security networks. [28] WPA algorithm utilize more secure encryption algorithm called as Advance Encryption Standard (AES). This protocol also uses better and advanced key distribution techniques, which help in improved session security to avoid eavesdropping.

2. Smart Grid

Smart grids play core part in a smart city regarding energy deployment and management. These are actually communicating instruments including sensors and communication networks that help in communicating data in real time [18]. When the data is shared in real time scenario among power generator, distributed resources, the service provider and the users, any information that is prone to attacks, that would take the system to failure. This will unfortunately lead to user's uncertainty and discontentment with the system. The threats are classified into four based on network availability, data integrity, information privacy and devices.

- Network availability

The network availability is targeted by Denial of Service (DOS) attack. These attacks attempt to delay, block or corrupt services by abusing information in the smart grid. It is evident that mostly of the smart grid use IP based protocols. As TCP/IP is open to DoS attacks, so such attacks are becoming huge problem in a smart grid.

- Data Integrity

Data like sensor value and control commands needs data integrity in case of smart grid. The main objective of data integrity includes defense mechanism for information modification through various

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

means such as message injection, message replay, and message delay on the network. For data integrity Cyclic Redundancy Code (CRC) or a Message Authentication Code (MAC) is used as a solution.

- Information privacy

Privacy of smart grid communication systems is important as it is the main concern and right of the consumers. Smart grid communications should take care of the privacy during communication in real time.

- Device

Smart meters are prone to physical attacks like battery change, removal, and modification. Moreover, functions including remote connect/disconnect meters and outage reporting may be used by unwarranted third parties.

Solutions for Smart Grid

The possible solutions for threats to devices in a smart grid include ensuring the integrity of meter data and maintaining meter securely. Moreover, for wireless networking, TCP/IP for smart grid networks is a better choice for Internet. Moreover, the M2M solutions prosed by IEEE including 802.11i, 802.16e, and 3GPP LTE should be used. For sensor networks various encryption standards should be adopted for authentication. Public key infrastructure (PKI) and managed PKI are also a good choice for smart grids security.

B. Governance Factors

The governance factors that influence and trigger the security issues include utility, health
sector, infrastructure, education, transport, etc. The biggest concern for the researchers is that a smart city though promises to provide all the ways to maintain whole infrastructure and management issues, but it's improper implementation can lead us to attacks and frauds. These malicious attacks and frauds can be very harmful to the core purpose of smart cities.

1. Threats to Critical Infrastructures

In critical infrastructures changing a single process in a critical system can cause delay or
loss of critical services. The main critical infrastructures include health care, industry and telecommunication. The implementation of critical infrastructure is mainly on IoT and Smart Grids. These two critical infrastructure need protection from malicious attacks that may cause crucial damage to smart cities and their promised services. The health sector is one of the most important type of critical infrastructure as if it is prone to security threats, it can not cause privacy concerns of a patient [21] but may also pose threats to his life as the critical information can be changed by the attacker.

2. Smart Mobility

Smart mobility causes privacy concerns as personal information disclosure could happen in collecting, publishing, and utilizing trace data. Some of the smartphone apps that provide services of smart mobility take mobile data and use trace analysis and data mining techniques. Moreover, the information sent and received from devices used in smart mobility infrastructure may subject to malicious attacks causing wrong traffic reports in satellite navigation systems.

3. Utility services

These are increasingly relying on smart grids that use bidirectional communication with the users in order to manage the distributed energy efficiently. Cloud computing also plays its role by providing features that are well suited for smart grid software platforms. Data security and privacy remain top concerns for utilities and the users that is playing a crucial setback in the adoption of smart grids. In order to save energy and utilities from malicious attacks, suggests that public key infrastructure (PKI) or managed PKI can be used to tackle security issues in smart grids.

C. Socio-Economic Factors

The smart city promises smarter economic growth as it provides services to enhance the banking, finance and business activities more efficiently. The social and economic factors in a smart city include communication, individual identity, banking and finance.

1. Banking and Ecommerce

The banking, finance and business are all part of smart economy that is a fundamental component of a smart city. It is most vulnerable to security threats as it can be attacked for personal financial use. The attackers also intend to sabotage the economy of certain organization, or a whole city.

2. Privacy

The privacy of individuals is a fundamental right that should be guaranteed in a smart city.

The individuals of a smart city use various services and communicate with each other through latest technology that is connected using heterogeneous networks and systems, which are the target for hackers who want to intrude in their personal privacy thus

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

depriving them from their personal right The privacy concerns linked with the social networking depend on the level of identification of the provided information by the individual, the receivers and the way it may be used. Those social networking providers that promise not to expose their user identities openly still may provide the required enough data to identify the individual's profile. [23] The IoT technologies with their security threats and solutions for smart city applications are listed in the following table 3.

TABLE III: IOT TECHNOLOGIES AND SECURITY THREATS FOR SMART CITY

Technologies	Smart City application	Security threats	Solutions
M2M	Smart Communication, health, governance, education	Physical attacks, protocol attacks, DoS attacks, privacy attack, Authenticated token attack	IEEE standard 802.15.1 802.15.4 802.15.11
Smart Grid	Smart energy, power, utility, smart appliances and smart home	Network availability attack, DoS, threats in Data integrity, message delay and replay, privacy attacks	Public Key infrastructure (PKI), AES for network, 802.11i, 802.16e
Smart Phones	Smart mobility, smart communication	Health and Spyware, location privacy, threats in social networking, malicious applications	Antivirus, firewall, secure API, authentication control.
Wireless sensor network	Utility, Health, Infrastructure, governance and commerce	DoS, threats in data integrity, unauthorized access, misuse of resource management	MAC, PKI, secure protocols, digital signature, symmetric cryptography

VI. CONCLUSION

The issue of information security in a smart city ranges over on a variety of aspects including social, economic, structural and governance factors. This paper provides a comprehensive overview on the threats, vulnerabilities and available solutions in order to facilitate much needed research in addressing the problem areas in smart city security. The technological factors are pivotal in deployment and maintenance of a smart city. In fact, technology is the driving force that establishes and maintains a smart city to deliver the promised services.

REFERENCES

[1] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the internet of things using big data analytics", Computer Networks, 2016.

[2] K. R. Kunzmann, "Smart cities: A new paradigm of urban development," Crios, vol. 4, no. 1, pp. 9–20, 2014.

[3] X. Nie and X. Zhong, "Security in the internet of things based on RFID: Issues and current countermeasures," in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, Atlantis Press, 2013.

[4] R. Pateriya and S. Sharma, "The evolution of RFID security and privacy: a research survey," in Communication Systems and Network Technologies (CSNT), 2011 International Conference on. IEEE, pp. 115–119, 2011.

[5] Boob T. N., Dr. Y.R.M. Rao," Violation of Building Bye-Laws and Development Control Rules: A Case Study, IOSR Journal of Mechanical and Civil Engineering (IOSRJMCE), Volume 2, Issue 4, pp 48-59, (Sep-Oct 2012).

[6] A.K. Evangelos, D.T. Nikolaos, and C.B. Anthony, "Integrating RFIDs and smart objects into a Unified Internet of Things architecture," Advances in Internet of Things, vol. 1, pp. 5-12, 2011.

[7] M. Shafie-khah, M. Kheradmand, S. Javadi, M. Azenha, J.L.B. de Aguiar, J. Castro-Gomes, P. Siano, and J.P.S. Catalão, "Optimal behavior of responsive residential demand considering hybrid phase change materials," Appl. Energy, vol. 163, pp. 81-92, 2016.

[8] Aggarwal, R. and Lal Das, M. (2012) RFID Security in the Context of "Internet of Things". First International Conference on Security of Internet of Things, Kerala, 51-56, 17-19 August 2012

[9] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, pp. 1645–1660, 2013

[10] Sommaya Madakam, R. Ramaswamy and Siddharth Tripathi, "Internet of Things (IOT): A Literature Review", Journal of Computer and Communications, pp. 164-173, 2015.

[11] M. Shafie-khah, M. Kheradmand, S. Javadi, M. Azenha, J.L.B. de Aguiar, J. Castro-Gomes, P. Siano, and J.P.S. Catalão, "Optimal behavior of responsive residential demand considering hybrid phase change materials," Appl. Energy, vol. 163, pp. 81-92, 2016.

[12] N. Neyestani, M. Y. Damavandi, M. Shafie-khah and J. P. S. Catalao, "Modeling the PEV traffic pattern in an urban environment with parking lots and charging stations," PowerTech, IEEE Eindhoven, Eindhoven, pp. 1-6, 2015.

[13] M. Yazdani-Damavandi, M. P. Moghaddam, M. R. Haghifam, M. Shafie-khah and J. P. S. Catalão, "Modeling Operational Behavior of Plug-in Electric Vehicles' Parking Lot in Multienergy Systems," IEEE Trans. Smart Grid, vol. 7, pp. 124-135, 2016.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. II, Issue IX, September 2016

[14] N. Neyestani, M. Y. Damavandi, M. Shafie-Khah, J. Contreras, and J. P. S. Catalao, "Allocation of plug-in vehicles' parking lots in distribution systems considering network-constrained objectives," IEEE Trans. Power Syst., vol. 30, pp. 2643-2656, 2015.

[15] M. Sen, A. Dutt, S. Agarwal, and A. Nath, "Issues of privacy and security in the role of software in smart cities," in Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, pp. 518–523, 2013.

[16] A. P. A. Ling and M. Masao, "Selection of model in developing information security criteria on smart grid security system," in Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on. IEEE, pp. 91–98, 2011.

[17] S. Goel, "Anonymity vs. security: The right balance for the smart grid," Communications of the Association for Information Systems, vol. 36, no. 1, p. 2, 2015

[18] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, "Smart cities built on resilient Cloud computing and secure Internet of Things," 19th International Conference on Control Systems and Computer Science (CSCS), pp. 513–518, 2013.

[19] Chen, X.-Y. and Jin, Z.-G. Research on Key Technology and Applications for the Internet of Things. Physics Procedia,561-566, 2012.

[20] W. Z. S. L. Gang Pan, Guande Qi and Z. Wu, "Trace analysis and mining for smart cities: issues, methods, and applications," IEEE Communications Magazine, vol. 121, 2013.

[21] P. Siano, G. Graditi, M. Atrigna, A. Piccolo, "Designing and testing decision support and energy management systems for smart homes", J. Ambient Intell. Humanized Comput., vol. 4, pp. 651-661, 2013.

[22] M. Parvania, and M. Fotuhi Firuzabad, "Demand response scheduling by stochastic SCUC," IEEE Trans. Smart Grid, vol. 1, pp. 89–98, 2010.

[23] R. F. Arritt, R. C. Dugan, "Distribution system analysis and the future smart grid," IEEE Trans Ind Appl., vol. 47, pp. 2343-2350, 2011.

[24] G. Zhabelova, and V. Vyatkin, "Multiagent Smart Grid Automation Architecture Based on IEC 61850/61499 Intelligent Logical Nodes," IEEE Trans. Indus. Elec., vol. 59, pp. 2351-2362, 2012.

[25] M. Yun, and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," International Conference on Advances in Energy Engineering (ICAEE), pp. 69–72, 2010.

[26] D. Corsar, P. Edwards, N. Velaga, J. Nelson, and J. Pan, "Short paper: addressing the challenges of semantic citizen-sensing," 4th International Workshop on Semantic Sensor Networks, CEUR-WS pp. 90–95, 2011.

[27] A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a service and big data," 2013.

[28] S. Bai, Y. Wang, and Z. Xue, "Research on security of wpa/wpa2 protocol," Information Security and Communications Privacy, vol. 1, pp. 106–108, 2012.

K.Harikrishnan is currently working as Assistant Professor in the Department of Electrical and Electronics Engineering at Sri Ramakrishna Engineering College, Coimbatore. He has a Bachelor's Degree in Electrical and Electronics Engineering in Odaiyappya College of Engineering, Anna University Chennai,2006, a Master's degree in Embedded Systems, Anna University of Technology Coimbatore, (2009). He has 7 years of teaching experience & has guided few UG projects. His research and teaching interests include in Embedded System Design, Microprocessors & Microcontrollers, Advanced Digital System Design. He has published many papers in International Conferences.

K.Balamurugan is an Assistant Professor (Senior Grade) in the department of Electrical and Electronics Engineering at Sri Ramakrishna Engineering College, Coimbatore. He is currently pursuing part time Ph.D. in Anna University, Chennai in the field of Torque and Ripple minimization of Industrial Machines. He procured his post graduate degree in Power Electronics and Drives from Kumaraguru College of Technology, Coimbatore and his under graduate degree in Electrical and Electronics Engineering from Muthayammal Engineering College, Rasipuram. He has a teaching experience of more than 9 years. He offers courses in the area of Circuit Theory, Control Systems, Digital principles and System Design, IC and Linear Integrated Circuits and Power Electronics. He is proficient in the application of Integrated circuits.