International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

Security Privacy & Threads in Smart City

[1]V.Ajith, [2]Mr.Vijaya Kumar .S

Abstract— Smart city opens up data with a wealth of information that brings innovation and connects government, industry and citizens. Cyber insecurity, on the other hand has raised concerns among data privacy and threats to smart city systems. In this paper, we look into security issues in smart city infrastructure from both technical and business operation perspectives and propose an approach to analyze threats and to improve data security of smart city systems. The assessment process takes hundreds of features into account. Data collected during the assessment stage are then imported into an algorithm that calculates the threat factor. Mitigation strategies are provided to help reducing risks of smart city systems from being hacked into and to protect data from being misused, stolen or identifiable. Study shows that the threat factor can be reduced significantly by following this approach. Experiments show that this comprehensive approach can reduce the risks of cyber intrusions to smart city systems. It can also deal with privacy concerns in this big data arena.

Keywords—hacking, security, smart cities, cyber cities, cities, cyber terrorism, cyber-attacks, cyber war, cyber criminal.

1 INTRODUCTION

Globally, policy makers are thinking about new urban concepts every day. Partly out of necessity; as traffic congestion, pollution and smog are seriously endangering living conditions and public health. And partly because state-of-the-art technological developments like the Internet of Things and Big Data analysis are providing new opportunities. These new urban concepts are commonly referred to as Smart Cities.A Smart City is a city where information technology and the Internet of Things are used to manage and control the city. This includes both their administration and the management of facilities such as libraries, hospitals and utilities and, most importantly, the public transportation system. Different sectors have been working on the Smart City concept in recent years - first and foremost the transport and traffic sector. But local government, health care, dirt management, water management and energy markets are also developing online services and applications that should help to realize a Smart City: A city that is cleaner, safer, more accessible and more attractive to citizens and businesses.

2 WHAT IS A SMART CITY?

What do people mean by the term 'smart city'? A casual search of the web turns up thousands of references to the term. Some define the smart city as an urban environment that is elegantly efficient, grander than the messy urban environments we live in today. For firms in the business of selling controllers, sensors, and servers—the technology to drive smart systems—the smart city is a new market for urban management. It is an urban form to be sold, resold, modified or augmented to make money. Many analysts and practitioners, however, are more modest in their definitions, limiting 'the smart city' to a few approaches that use publicly available data to solve discrete problems, such as waste management and traffic control. The authors in this special issue have different perspectives but define the smart city by two essential attributes. First is the use of technologies to facilitate the coordination of fragmented urban sub-systems (for example, energy, water, mobility, built environment). Becoming 'smart' by subsystem improvement is assumed to be Associated with new employment opportunities, wealth creation and economic growth. In a second and more futuristic definition, smart cities are urban places where they lived experience calls forth a new reality. There are, in fact, few finished examples of Greenfield sites that represent full deployment of the idea. As Carvalho (2015) details, even the less encumbered Greenfield models such as Song do or Mazda City, took so long to roll out that the political will deteriorated and the original impetus slackened across political cycles. As Shelton, Zook and Wiig describe, the fully formed Greenfield smart city will be the great exception (Shelton et al., 2015). Most smart cities are about fixing things by adding off-the-shelf technology to existing functions such as transportation planning to make existing systems more efficient, predictable and, in rare cases, redeploy able with re-programming. In the vast majority of cases, smart cities are about renovation rather than about building wholly new urban environments and, as such, they will all be different because of the exigencies of municipal budgets and political choices.

3 SMART CITY ENTITIES

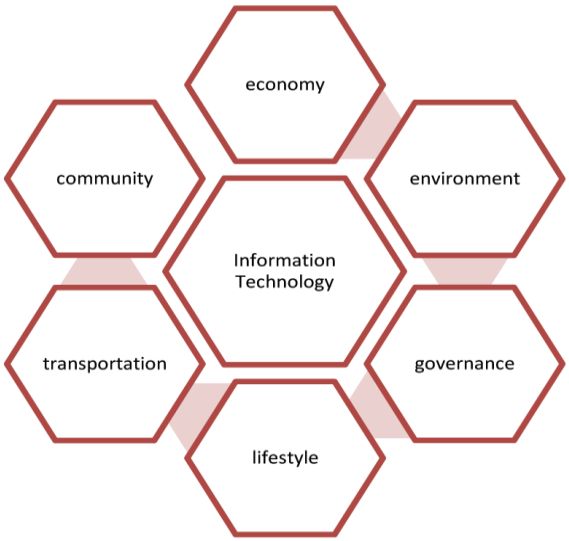
3.1 SMART GRIDS

Smart grid technology is changing the way traditional power grids operate by reducing energy demands, global warming and consequently, utility costs. Consumers are required to share information about their energy consumption with their utility providers, over communication channels using smart meters. The interconnection of multiple smart meters and computerized infrastructure of the grid makes them vulnerable to several network based attacks Data from smart grid devices can be essential for studying energy consumption patterns and supply/demand management. Traditional data management applications are not designed to handle large scale data generated by the grid. Cloud computing isan appropriate choice that can be leveraged to store and process such large volumes of data (Bera et al., 2015). Data can also be used for detecting anomalous behavior in smart grids and can assist in forensic investigations. Anomaly detection techniques applied to data from different IoT components operating

- [1]*V.Ajith, II-Year MCA, Priyadarshini Engineering College, Vaniyambadi, Email: vajith113@gmail.com*
- [2]*Mr.S.Vijayakumar, Associate Professor& HOD, MCA, Priyadarshini Engineering College, Vaniyambadi, Email: Vijayviswak@gmail.com*

in a smart grid can detect compromised devices and protect smart grid operations. Smart grid threats can be categorized into those that affect: network availability, data integrity and information privacy. Devices such as smart meters and IoT devices within a consumer's household are located in physically insecure locations and can be exploited by an adversary. Since the grid maintains a two-way communication channel with multiple intelligent smart grid devices and the Cloud, these exposed devices create numerous entry points for an adversary to penetrate the smart grid, and also expose smart grid data stored in the Cloud to various security threats. Consumption patterns could also be utilized by an adversary to extract household information such as the number of individual slaving in a house, and the various types of appliances in use (Jokaret al., 2016). Another challenge to privacy of smart grid data is the ownership and accessibility of consumer data stored in the Cloud. Jokar et al. (2016) suggest using anonymization of the data to hazeout attribution of any traits to a particular customer mart grids are also vulnerable to attacks that can affect the timely delivery of messages between interconnected systems, which is critical to the successful operations of the grid.

From the ethereal to the pragmatic, Rob Godspeed suggests smart city definitions bifurcate, with one strand emphasizing urban and economic development, while the other focuses on government's use of technology for public sector operations (Good speed, 2015). The limits of agreement around the concept arise in part because, as with prior moments when the rate of economic growth has stumbled, economic actors look for new markets to deploy existing technology. They grope for a synthesis that will kick off a sustained round Of job generation and capital investment. For example, one progenitor of the smart city, the 'intelligent city' dates back to the 1980s, another period of sluggish economic growth, when, following on the heels of the early 1980s banking crisis, economic development professionals Searched for another source of lift in the economy.



4 Security concerns and threats

Security concerns and threats although much of the publicity about Internet security has focused on the Potential risks to consumers who use credit cards to make purchases electronically, payment fraud is also a major threat to Internet-based merchants (Murphy, 1998). Fraudulent or non-creditworthy orders account for as much as one-sixth of all attempted purchases on the Internet. Security threats not only consist of break-ins and technology disturbance, but also stalking, impersonation, and identity theft are serious issues that everyone should be concerned about (Janal, 1998). Computer hacking is another serious problem. Hacking can be either a benign or a malicious activity.

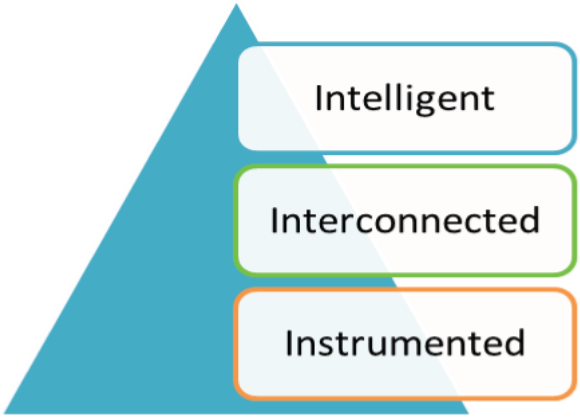
5 E-mail concerns

Electronic mail will continue to gain popularity in years to come. Corporations and individuals are nowusing e-mail as a major means of communication. Like other technological developments, e-mail has both advantages and disadvantages, along with controversy (Botham, 1996). E-mail privacy has been an issue of considerable debate. Despite new developments in encryption and despite new legislation, e-mail privacy has proved to be of major concern to the users. Over the past few years there has been a rising concern over the apparent increase in unsolicited e-mail (junk e-mail), otherwise known as spam. This process of mass distribution of unsolicited e-mail advertisements has become much more common and generally accepted and tolerated, if not loved, because of many powerful corporations. Some people have estimated the amount of spam flowing through the Internet to be up to 30 percent of all e-mails, which is an indication that spam is one of the major concerns today that IT users have to deal with. As expected, the governments of the
Nations are making efforts to relieve the IT users' concerns. In the USA, there is statutory privacy protection by the Electronic Communications Privacy Act, but this act is limited because an employee is not able under the statute for reading an employee's e-mail if one of the parties to the communication consented to the monitoring. Many companies adopt e-mail policies which employees sign, agreeing that they consent to such monitoring on an ongoing basis. Again, employers are allowed to monitor e-mail if there is a legitimate business reason for the monitoring. In essence, a company that provides an e-mail service can monitor communications in order to protect itself, such as in cases where the company believes it is being defrauded. Organizations are increasingly adopting policies which address e-mail privacy concerns. Of course, there are competing interests at stake.

6 Information Security In A Smart City

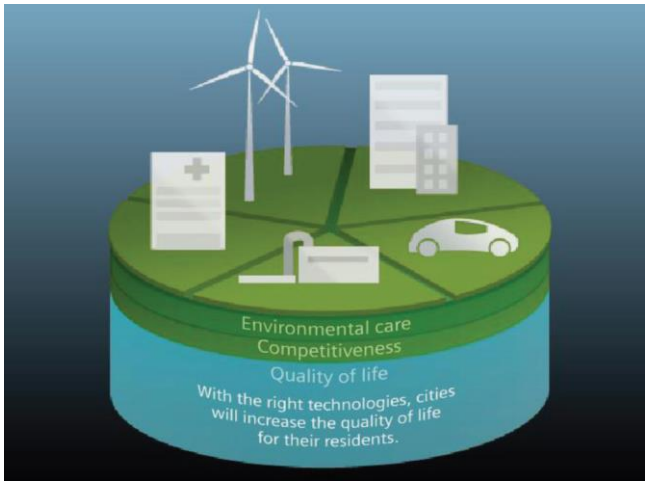
The security and privacy of information in a smart city has been interest of researchers. The reason behind it is that, in order to ensure the continuity of critical services like health care, governance and energy/utility issues in a smart city, the information security must be fool proof. The factors that are taken under consideration in order to

identify the issues in information security in a smart city include governance
Factors, social/economic factors and most importantly economic factors. These factors are elaborated in the Figure (2). The researchers identify, explain and propose solutions to the information security issues by considering the mentioned factors. Most of the research work discuss the components and architecture of a smart city and then describe solutions for the security and privacy concerns.



- Intelligent traffic solutions,
- Green buildings,
- Water management, and
- Smart grid infrastructure

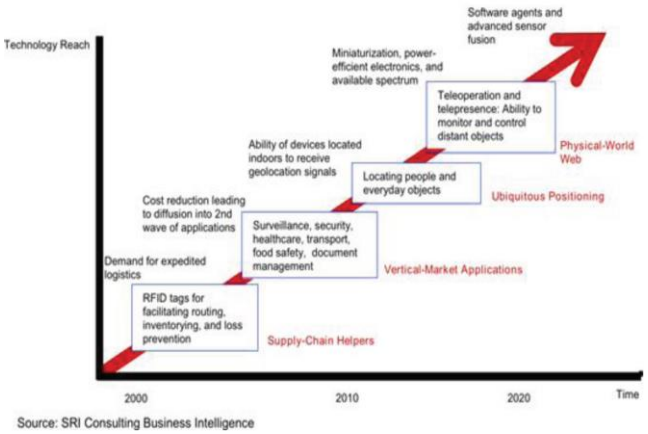
A case study of New York City initiatives demonstrates that adaptability is one of the most important
aspects of neighborhoods which are the building blocks of communities (Siemens - a). An illustration
of this concept is provided in Siemens website (Siemens - b) and shown in Figure 3 - Siemens
Sustainable City which leads an increase in the quality of life.



In a variation from IBM and Siemens, we note that CISCO's approach is referred to as "Smart+ Connected Communities" with a focus on transformation of physical assets in communities into inter-connected ones as the basic enabler for a smart city. In Figure 4 - Elements of CISCO's Smart+ Inter-connected Communities. A brief description of CISCO's rationale can be summarized as follows:

"As world populations shift to urban areas, community leaders are pressed for answers to related problems. These include overcrowding, pollution, budget and resource constraints, inadequate infrastructures, and the need for continuing growth. Cisco Smart+ Connected Communities solutions use intelligent networking capabilities to bring together people, services, community assets, and information to help community leaders address these world challenges. By connecting the unconnected, we can do amazing things to address these real world challenges and create a more sustainable environment." (CISCO).

An important component of smart cities is the home appliances and the power connectivity which has been reference earlier as part of the smart grid initiatives. It was reported that in an interesting business collaboration, GE & Samsung have joined forces to revitalize Korea's Smart Grid Industry(Chung, 2010). The strength of this collaboration lies in the fact that they include the 2-way connectivity needed in a smart grid and the smart appliances that both companies can produce. So, this connects the home to the energy suppliers and enables what is now referred to as the



Source: SRI Consulting Business Intelligence

7 Cyber Attacks On Cities

All technologies used by cities plus all the associated cyber security problems that were previously described open the door for several possible cyber attacks. Each new city technology or system creates a new opportunity for cyber attackers. Let's discuss in depth some of the key

technologies and systems that together make up the smart city's complex attack surface:

- Traffic Control Systems
- Smart Street Lighting
- City Management Systems
- Sensors
- Public Data
- Mobile Applications
- Cloud and Saas Solutions
- Smart Grid
- Public Transportation
- Cameras
- Social Media
- Location-based Services

8 Traffic Control Systems

Last year, a research team from University of Michigan and I independently proved that traffic control systems could be easily hacked.27, 28 The University of Michigan research found that some Economize devices were used without any encryption for communication between traffic control systems and traffic lights, traffic controllers, and so on, allowing an attacker to directly change traffic lights. 100,000 intersections in the US and Canada could be affected. In my research I found that Senses Networks devices didn't have any encryption, any authentication, or any security at all. It was possible to feed traffic control systems with fake data making them accept incorrect options when setting configuration and timing on traffic lights, ramp meters, traffic signals, and so on. It was possible to fully compromise the sensors and even to create a firmware update worm. 200,000 vulnerable sensors deployed worldwide were affected. We still don't know if these vulnerabilities were patched. If they were, we don't know how the patch addressed the vulnerability and whether the patches actually were applied. Cities can't easily detect if someone did something malicious like updating firmware with backdoors. I had an interesting discussion with someone from the US Department of Transportation (US DOT), who wasn't really worried about these vulnerabilities since he said "we have worse things to worry about." I couldn't fight that argument but it shocked me to know that US cities are vulnerable to worse attacks on traffic control systems that the one I discovered.

9 Smart Street Lighting

Wireless street lighting systems are being deployed in many cities around the world. Most systems use wireless communications and have the encryption related problems previously described. Attacks on smart street lighting systems are not complex and can have big impact by causing street blackouts in large areas. For example, there exists a scenario where a street blackout could affect an entire island in the US Virgin Islands where a wireless street lighting system was implemented I have tried to get my hands on the specific devices used in the US Virgin Islands, resulting in about a dozen calls and emails with the vendor, who promised to send me a quote for the devices but did not send it. Why is it to hard to acquire such equipment? Why the vendor wouldn't sell it to IO Active? There are also wired solutions using Power-line Communication (PLC) technologies that also could have the encryption problems that were already mentioned.

10 City Management Systems

Every city has hundreds of systems to manage different services and tasks. Hacking these systems would give an attacker a lot of options to cause harm. Just as simple software bugs can create significant harm, manipulating simple information could also have a seemingly oversized security effect. imagine if an attacker can intentionally trigger those bugs and with some planning, get an even bigger impact. For instance, an attacker could manipulate map information and work orders to send city or contractor workers to dig a hole over gas or water pipes or communication cables, with the intention to damage those facilities. After all, this has already happened in the past by mistake several times. On June 7, 2010, a 36-inch gas pipeline explosion and fire in Johnson County, Texas, was caused by workers installing poles for electrical lines. One worker was killed, and eight were injured. Due to confusion about the location and status of the construction work, the pipeline was not marked beforehand

11 Sensors

Smart city systems rely heavily on sensor data to make decisions and take action. Most sensors use wireless technologies that are affected by the types of security problems already mentioned. Attacks that involve compromising sensors and sending fake data can directly affect systems since decisions and actions will be based on fake data. This could have great impact depending on how the affected systems use the data and interact with other systems. Attackers could even fake an earthquake, tunnel, or bridge breakage, flood, gun shooting, and so on, raising alarms and causing general panic. An attacker could launch a nuisance attack by faking data from smell or rubbish level sensors in empty garbage containers, to make garbage collectors waste time and resources. Keep in mind that many systems and services from cities rely on sensors, including smart waste and water management, smart parking, traffic control, and public transport. Hacking wireless sensors is an easy way to remotely launch cyber attacks over a city's critical infrastructure.

12 Public Data

Public data (open data) is available to attackers, sometimes in real time. This data can help them determine the best timing for attacks, schedule attacks, create attack triggers, coordinate attacks, and so on. Attackers don't need to act blindly; they can act precisely, relying on real data. For instance, attackers can identify exactly when a bus or train is arriving. They can see when traffic is heaviest, when more people are gathering at a location, and so on. Also, information about the technologies in use in cities is often available since

governments have public lists of technology providers and contracts.32 Sometimes vendors will highlight case studies for cities that have been deployed.33All of this gives attackers a lot of detailed information to work with.

13 Mobile Applications

Mobile applications are affected by common security vulnerabilities which could allow attackers to perform a variety of attacks, from simple Man in The Middle (MiTM) 34 attacks to more complex attacks. Attackers could also target mobile application development companies or just target the data that feeds the applications. Mobile applications are an important target since cities' citizens will make decisions and act based on information from those apps. Hacking mobile apps has direct impact on citizens' behavior. For instance, if the public transport app is showing a delay on a bus, a citizen could choose to travel to work by car; if the same decision is taken by hundreds of people in high density area, the result is a traffic jam, which we can think ofas a city DoS.

14 Cloud and SaaS Solutions

City servers and cloud infrastructure are exposed to common Distributed Denial of Services (DDoS) attacks. Severs and cloud infrastructure are cheaper targets for cybercriminals or cyber terrorists. Also, when in use, Software as a Service (SaaS) could allow attackers to hack a single service provider and then launch attacks against many cities at same time. Cities should consider the security implications of SaaS solutions as well as their functionality.

15 Smart Grid

Energy is the life line of a city; without energy there is no smart city. Last year, researchers Alberto Garcia Illera and Javier Vazquez Vidal at Black Hat Europe demonstrated it was possible to black out big city areas by manipulating smart meters35 exploiting encryption problems in Power-line Communication (PLC) technologies. This is not new; years ago Mike Davis of IO Active created the first proof-of-concept worm for
The smart grid.36 Attacks on a smart grid could be devastating, causing millions of dollars in losses and even loss of life.

16 Public Transportation

Citizens use public transportation information systems daily to know what time some transport is scheduled to arrive or depart, whether to expect delays, etc. By just by displaying incorrect information by manipulating public transportation information systems, it's possible to influence people's behavior to cause delays, overcrowding, and so on. For instance, by faking a delay in a subway line, attackers can influence people to move to another line, overcrowding it. Also an attacker could target payment systems. If payment systems don't work, people might ride for free or thousands of people could jam customer service counters and hotlines with complaints.

17 Cameras

Cameras are becoming more widely used in most cities around the world. Traffic and surveillance cameras are the eyes of the city and by attacking them, attackers can make cities blind. Our research has shown that DoS attacks on these devices are not difficult and that these attacks are very effective. It is not always possible to remotely restart cameras. In addition, DoS attacks can be made persistent by modifying firmware or exploiting vulnerabilities. Usually cities deploy hundreds of cameras of the same brand and model. This makes attacks easier since any vulnerability will affect all cameras in the city. Some of these cameras are wireless and suffer from the problems already described for wireless communications such as no encryption, weak encryption, and so on. Recently Kaspersky Labs researcher, Vasilis Hiuorios, found that police surveillance cameras were vulnerable and easy to hack

18 Social Media

Social media can be used as an amplification platform for attacks. We saw this in recent high-profile company hacks. For instance, attackers can increase the impact of an attack by causing panic in a population. If just one simple attack is real, then a bigger attack can be promoted. Even if promoted attack never happens, it will scare people. Every day that such a problem persists, it will grow and incite increasingly angry citizens. Attackers know this and can play with social media perceptions at will.

19 Location-based Services

Many services are location-based, which means GPS spoofing and other attacks are possible. People get real-time location information, and if the location is wrong, then people will make decisions based on incorrect information. The nature of the impact depends on the extent to which a city relies on the services affected.

20 Recommendations

The following are just basic, general recommendations to reduce problems. Much work is needed, but cities can get started using these steps that can make a big difference in the current situation:

• Create a simple checklist-type cyber security review. Check for proper encryption, authentication, and authorization and make sure the systems can be easily updated.

• Ask all vendors to provide all security documentation. Make sure Service Level Agreements include on-time patching of vulnerabilities and 24/7 response in case of incidents.

• Fix security issues as soon as they are discovered. A city can continuously be nder attack if issues are not fixed as soon as possible. For instance, if a traffic control system is hacked and not quickly fixed, it will continue being hacked over and over again and turn the city into chaos.

• Create specific city CERTs that can deal with cyber security incidents, ulnerability reporting and patching, coordination, information sharing, and so on.

• Implement and make known to city workers secondary services/procedures inase of cyber attacks, and define formal communication channels.

• Implement fail safe and manual overrides on all system services. Don't depend olely on the smart technology.

• Restrict access in some way to public data. Request registration and approval for using it, and track and monitor access and usage.

• Regularly run penetration tests on all city systems and networks.

• Finally, prepare for the worst and create a threat model for everything

21 Conclusion

The current attack surface for cities is huge and wide open to attack. This is a real and immediate danger. The more technology a city uses, the more vulnerable to cyber attacks it is, so the smartest cities have the highest risks. It's only a matter of time until attacks on city services and infrastructure happen. It could be at any moment. Actions must be taken now to make cities more secure and protect against cyber attacks. It's extremely important: Technologies used by cities must be properly security audited to make certain that they are secure before they are implemented. To fail to do so is reckless. When we see that the data that feeds smart city systems is blindly trusted and can be easily manipulated, that the systems can be easily hacked, and there are security problems everywhere, that is when smart cities become Dumb Cities.

References

[1] ABI Research. (n.d.). Smart Cities. Retrieved February 13, 2013, from http://www.abiresearch.com/research/service/ smart-cities/

[2] Bartol, A., Hernandez-Serranoy, J., M, Soriano, M., Dohler, M. A., & Barthel, D. (2011). Security and Privacy in your Smart City. Proceedings of Barcelona Smart Cities Congress. Barcelone, Spain.

[3] Chui, M., Löffler, M., & Roberts, R. (2010, March). The Internet of Things. Retrieved February 14, 2013, from McKinsey Quarterly: http://www.mckinseyquarterly.com/The_Internet_of_Things_2 538 Chung, Y. (2010, May 26). GE & Samsung's Collaboration brings the Spotlight back to orea's Smart Grid Industry. Retrieved February 14, 2013, from Korean Insight: [4] http://www.koreaninsight.com/2010/05/ge samsungscollaboration- brings-the-spotlight-back-to-koreas-smart-grid-industry/

[4] CISCO. (n.d.). Smart+Connected Communities. Retrieved February 14, 2013, from http://www.cisco.com/web/ strategy/smart_connected_communities.html

[5] Duhigg, C. (2012, February 16). How Companies learnyou're Secrets. The New York Times Magazine. El Khayat, G. A., Mabrouk, T. F., & Elmaghraby, A. S. (2012). Intelligent serious games system for children with learning disabilities. CGAMES (pp. 30-34). Louisville, KY: IEEE.

[6] Elmaghraby, A. S., Kumar, A., Kantardzic, M. M., & Mostafa, M. G. (2005). A Scalable Pricing Model for Bandwidth Allocation. Electronic Commerce Research, 5(2), 203-227.

[7] Elmaghraby, A. S., Méndez, A., García Zapirain, B., Sheta, W., & el Shehaby, S. (2012). CGAMES (pp. 35-38). Louisville, LY: IEEE.

[8] Elmaghraby, A., Graham, J., & Turner, M. (2011, December). Kentucky's Smart Grid Roadmap. IEEE SmartGrid. Piscataway, NJ, USA.