Security in Modern Smart Cities: An Information Technology Perspective

Tanzeela Jameel*, Rukhsana Ali†, Shumaila Farhan‡
* Faculty of Social Sciences, University of Balochistan, Quetta, Pakistan.
† Faculty of Humanities and Social Sciences, University of Jyväskylä, FI-40014 Jyväskylä, Finland.
‡ Institute of Science, Technology and Development, Mehran University of Engineering and Technology, Jamshoro, Pakistan.
Email: tanzilajameel26@gmail.com

Abstract

In a modern and big city, the security system is not a single layered single module system. Instead, it consists of many layers with autonomous subsystems which are capable of interfacing reciprocally in an efficient and coordinated way horizontally and vertically. The design of such indigenous subsystems and ensuring tight interaction between them taking into account high usability and resource utilization is not a simple task. In this regard, this article provides a comprehensive overview of the security systems in smart cities. We begin by introducing trends and key stakeholders in smart cities. Next, we provide examples of mass surveillance systems in developed countries like USA, UK, and China. Finally, we highlight some of the major challenges in complete realization of smart cities. The security aspects discussed in this study can be beneficial in designing future smart cities.

Index Terms

Autonomous systems, Mass surveillance, Smart cities, Security

I. Introduction

A new era of technology has presented the solution to city security problems in the form of sensor fusion, machine learning, and artificial intelligence. But this also has its own share of challenges ranging from technical to financial. Sensors installed at all these locations would generate a colossal amount of data for processing and analysis and that is the core challenge faced by the cities around the world. Putting a surveillance camera on a roundabout would not stop any crime or terror activity by its own. What it sees, record and send to the command center must be analyzed as well if it has to contribute in a responsive security system for the city. It is obvious that protecting the data generated by sensors and the networks which carry this data from sensors to command centers itself is a challenge.

It is not the internet alone but the IoT (internet of things) which is the future of the city security system. IoT builds a network of all interconnected devices in the city [1]. An IoT based IP network is required to connect all the devices and sensors to the internet or another high-speed intranet for analysis, storage, and backup. Such a the network would naturally demand a considerable amount of investment in existing communication networks so that they can handle a large amount of data.

Most important sites in any city are its egress and ingress air, land and sea routes. It means airports, seaports, bus terminals along with intercity roads form a security perimeter in any city. And if the population of that city is more than 100 million, then this broad perimeter security pose a serious challenge for the city administration. Overcoming this challenge means only securing physical axis of human security. Ensuring smooth traffic throughout the city, effective policing and security of critical infrastructure in the city like hospitals, energy grid, water supply lines, gas distribution grid, electric feeders, banks, and educational institutions etc. Each one these elements demand protection particularly in countries like Pakistan where cities are expanding at an exponential rate without any city planning for the long-term implication of such rapid urbanization [2], [3].

Motivated by aforementioned developments, this article discusses the crux of security in smart cities. Especially, from information technology point of view, security becomes naturally a challenging job for system managers and network managers. Identifying attack and defense layer in the security system is critical for data security and system integrity. Therefore, this article aims at identifying some latest trends and highlight the major challenges associated with securing the future smart cities.

The remainder of the paper is organized as follows. Section II discusses smart security framework, while Section III presents some key stakeholders in the development of smart cities. Then, Section IV provides a comprehensive discussion on key technological trends in smart cities which is followed by Section V that reviews mass surveillance systems. In Section VI, some prominent challenges are highlighted for the realization of smart cities. Finally, Section VII concludes this work.

II. Basic Smart City Framework in Action

Safe security systems are implemented based on a layered framework. Each layer in a typical framework represents a specific role and scope within the system. Every modern smart city project has some core layers presenting the mandatory functionality [4]. A typical layered framework of a smart city system is shown below.

h

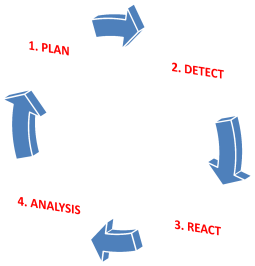

Fig. 1. Stages of development of smart cities.

- **Application Layer**An application layer infrastructure is present on this layer. It connects the core network traffic to the specific applications designed for a corresponding first responder like a firefighter, ambulances, police, etc.
- **Network Layer** This layer act as an integrator between application and sensors. It is usually comprised on the mission-critical network. It connects different communication technologies like 2G/3G/LTE etc. with IP based core network.
- **Sensory Layer** This layer represents all the sensors and monitoring devices like CCTVs installed throughout the city [5].

A. *Basic smart city framework*

This is a basic level smart city framework layer model and more complex models can be built based on it. The complexity of a smart city framework depends upon the required functionality apart from core functions like surveillance and central command and control [6]. Below is an operational cycle of a basic level smart city project with core functionalities.

Output at each stage of the framework provides the input for the next stage, as illustrated in Figure 1. This is essential for the framework to grow. There are 4 stages; Plan, Detect, React, Analysis.

1) Plan: Planning phase includes policy and design level decisions to ensure that responsive procedures, correct routing rules, ACLs and information workflow are being implemented. Any variable required is integrated into the framework at this stage [2], [7].

2) Detect: In this stage, sensors at the sensory layer detect some abnormal behavior or pattern in traffic or detect some law and order incident and the information is passed to the command and control center using securing communication channels connecting the entire system together.

3) React: The role of this stage is to provide the best line of action in the given scenario. It happens at the command and control layer of the framework.

4) Analysis: At this stage, logs are maintained for each action for future review so that any shortcomings in the system can be addressed at the planning level during the next system-wide review.

Usually, a smart city framework contradicts sharply with the enterprise architecture model. smart city frameworks are built keeping in mind the availability of open architecture with a potential of integration of multiple heterogeneous systems. This completely changes the stakeholder list. A comparison between enterprise and open architectures is shown below.

	Enterprise Architecture	**Open Architecture**
Organizations: LEA, Fire fighter, Ambulance services	Many	Many
Specific Requirements: Crisis management, surveillance, C&C, intelligent analysis	Many	Many
Technologies: Sensors, networks, servers, databases, Big Data etc.	Proprietary solutions	Many
Integrator/ Provider: System integration services for vertical & horizontal communications	Single Enterprise involved.	Many
Stakeholders: Sources of input as suggestions	Limited	Many

TABLE I
ENTERPRISE AND OPEN ARCHITECTURES MODEL.

This comparison proves that it is almost impossible for any single technology firm to provide the entire system on its own so open architecture is the only logical choice for any city to build a smart city architecture blueprint as the requirements and complexity dictates towards an obvious choice between two types of possible architectures.

III. STAKEHOLDERS IN SMART CITY

Based on this discussion in the last section about the framework architecture, the following list of key stakeholders emerged.

A. *Regulators*

The regulatory authorities define the policies and regulations which govern the entire smart city system along with its critical aspects like quality, data security, responsiveness, and reliability etc.

B. Network and telecom providers

These organizations build and provide the backbone of all the communication systems in the city for data transmission. It includes both private and public enterprises. The robust and well-established infrastructure fulfills the heavy bandwidth requirements of a smart city project via legacy 2/3G technologies or emerging LTE and 5G wireless technologies [8]–[10]. These operators use copper and fiber optic channels to form their backbone networks which enable them to provide high-speed data traffic.

C. Technology providers

These actors are responsible to develop and provide technologies required to fulfill the functionality of Network Layer in a smart city framework. Surveillance systems, detectors, sensors of different types are provided by technology providers. Their the role is critical in the overall quality and reliability of the smart city the project as they are responsible to provide management software for video surveillance, network communication equipment, and data storage solutions. For more advanced framework their role elevates further. In that role, they supply the video analytics systems like ANPR, intrusion detection system (IDS), video management software, facial recognition system, switches, routers, storages in SAN, NAS, SATA etc.

D. Channels

Channels actually install, commission, test and maintain all the hardware across the smart city system. They are firms working in close coordination with technology providers and OEMs respectively.

E. Users

Government departments, businesses, commercial and domestic entities mainly drive the demand for the reconnaissance arrangements. They determine the expectations of a system by laying down the functional and technical requirements based on the security policies at city, province and national levels.

F. Robust technologies

Today, a robust security system incorporates a range of different technologies for data generation, transmission, storage, and analysis. So it is obvious that for all these heterogeneous amalgamations of technologies to work, there must be a mechanism so that different devices can talk to each other, as shown in Figure 2.

Selection of technology at each step of designing a smart city system is critical as it is the technology which in the end is going to make the difference between law and crimes; peace and instability [11], [12]. Law enforcement agencies would be able to respond earliest if the enabling technologies which the system is based on are interacting with each other at an optimal level. To make this happen, careful technology planning is critical in the conception of any citywide security project [2].

Before analyzing some of the contemporary and emerging smart city technologies, it would be prudent to take a high-level look at the overall technology trends in smart city domain [13], [14]. This knowledge will help in deciding which kind of technology to adopt, what kind of data analytic services to choose and what are the options in terms of selecting technologies for making the entire system secured.

IV. Key Trends in Smart City Technologies

There have been three key trends emerging in the smart city technologies.

1) Transition towards wireless communication
2) Advances in cloud computing, machine learning, and intelligent data analytics
3) Evolution of smart technology concept in city security systems

Transition towards wireless communication

Wireless communication has emerged as unavoidable reality in mobile and tablet era. Wireless communications today connects billions of devices around the world. Developments of new wireless standards and their integration with existing wire-based systems have enabled the rapid growth of wireless communication. Long Term Evolution Solutions (LTE), City Clouds, Machine to Machine communication (M2M), Wireless Security protocols (WPS etc.) and IP stack services etc. are just a few of the technologies which have changed the communication landscape. Now, all the stakeholders involved in the development of a smart city project will be able to connect with each other while being mobile. This has reduced the time taken for data transmission, processing, and decision making. Now LEAs around the world use wireless equipped handheld devices for obtaining information about anyone from a number of databases residing on remote servers at distinct locations.

IP technology in video surveillance has enabled police to install IP cameras at locations where previously it was not possible due to the lack or absence of required network cables. Today, through IP technology, cameras can be installed immediately and effectively while also providing footage to multiple users across numerous remote locations.

Fig. 2. An illustration of connected sectors in smart city

A. Growth of Cloud Computing, Data Mining, and Analytics

Cloud computing allows large data storage and retrievals on a fast speed using virtual hard drives in their clouds. Computing clouds are usually connected with core networks around the world making them the obvious choice for data storage and processing. Cloud architecture has enabled the technology firms, individuals and governments to access their data from any location while saving the cost and space on own physical servers. This arrangement also decreases the traffic load on the own network. Data mining and analytics are emerging domains in data analysis. These technologies are helping governments with key data insights to interpret multiple scenarios from multiple vantage points in dramatically less time [15].

B. Integration of Smart Technology

Smart technology envisions the integration of all sensors, all people, machines in an intelligent way in an ecosystem like environment. To achieve this, efforts are being made to make the devices, people, and buildings smarter. Internet of Things (IoT) is a major development in this regard. Smart technology is already present through the aid of smartphones, contactless payments, near field communication (NFC), integration of smart cards with biometrics etc [16]. Once implemented completely, this technology is going to change the operational nature of smart city systems completely. Thought IoT multi fold information about each individual will be available to a lot many attributes of his life. IoT despite its benefits would complicate the architecture of a smart city system and there exist a number of caveats as technology firms around the world are trying to make it a reality [17].

V. Mass Surveillance System as counter Strategy

9/11 will be remembered as a watershed incident which made the world realize that the threat of mass terrorism is real and close. Security and surveillance emerged as a top priority in world capitals and the result was a culture of mass surveillance to monitor masses along with some other measures which were devised to track the communication and movement of individuals. Below is a brief description of these measures.

A. USA

In post 9/11, the world scrambled to enhance the security for larger urban centers. New departments were established in the US and new travel rules and regulations were made to plug the loopholes in immigration systems. Two of the major steps taken in the most advanced nation, US. One was the rapid development of a surveillance system by NSA to track Al-Qaeda

on the American soil. Secondly, social media giants like Facebook, Twitter, YouTube, Skype, and Google began to cooperate with NSA by turning over sensitive user information. Both these initiatives initially met with severe criticism as these violated personal liberties and the US constitutions. A new wireless surveillance unit was established in FBI as well with the core mission of developing new technologies for police and other law enforcement agencies to eavesdrop on the Internet and wireless communications of American citizens [18].

These overtures despite some criticism ensured the security of US cities and thats why till date no incident like 9/11 ever took place.

B. UK

Like 9/11, London witnessed horrific terror incident when, on 7/7/2005, four bombs carried by jihadi suicide bombers exploded on tube trains and a bus in London, killing 56 people including the attackers. This was the beginning of a new era of surveillance in the UK. Right now, there are more than 12,000 video surveillance cameras in London Underground alone. London authorities track criminals and terrorists using these cameras. The video surveillance system is callable of monitoring sensitive areas in real time. Like the USA, in the UK too, police was given special powers after 7/7 allowing it to keep terror suspects under its custody for four weeks without charging them. The UK also allowed it secret service to snoop on citizens internet data like happened in the US after 9/11. In 2015, it was revealed that a total number of installed cameras in London could be around 6 million.

C. China

China overhauled its city surveillance system in 2012 and achieved 100 percent coverage of Beijing city in 2015. Though no constitutional changes like US and UK were made in China after the installation of the surveillance system, the number of the police force has been increased in the capital. All cameras are controlled by Beijing's Public Security Bureau where activities of masses throughout the city are monitored and on detection of an anomaly on the field, troops are directed to rush to that location. Beijing is now considered among the cities with a top number of surveillance cameras installed.

D. France

France has implemented a mixed security approach comprising high-tech technologies along with low-tech legacy security measures. For instance, after deadly bombs were stashed inside sidewalk dustbins, the city removed all public waste containers and replaced them with models that used transparent bag.

Major tasks about Paris' security rest with the foot soldiers patrolling the street of the city who are being aided by less obtrusive security apparatus: the citys sophisticated video-surveillance technology. Video surveillance set up in Paris houses one of the most advanced Network Operation centers from where video surveillance is analyzed at a real time. All these examples show that video surveillance has been the most sought-after security solution around the world after the 9/11 incident. There exists a considerable pool of problems with these surveillance systems.

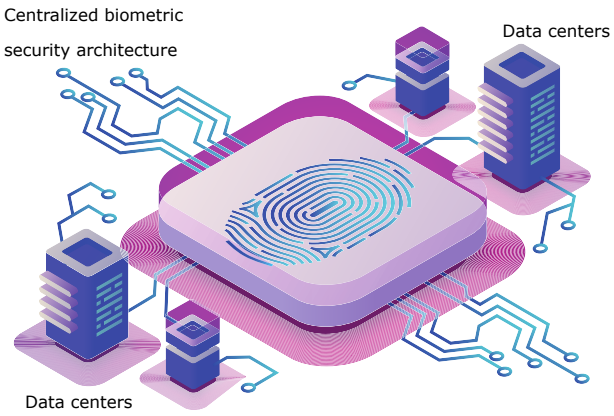

Fig. 3. Centralized biometric architecture.

VI. Challenges in Smart City Projects

Every city on the world map is different from any other city. Cities are different in terms of their population and area sizes, they are different in their demographic diversity, they are different with respect to their cultural values. They are also different in the level of social inclusion and economic viability. These are major differences which pose an extremely daunting challenge for the security architect to design a city-wide security system. But the challenges faced by any smart city project

are not limited to these differences alone. There are broader issues which need to be addressed first in order to make any smart city system work the way it was intended to do. Developing nations are particularly vulnerable to a series of challenges in implementing smart city projects. Below is a detailed analysis of these problems which may hinder the progress on smart city projects in developing nations and maturing cities.

A. Policy Level

Institutional disconnect, political interventions, and weak administrative hierarchical structures always lead to poor governance and policymaking. No single state organ can overcome security challenges of today hence a multi-level coordinated governance model must be followed which can provide a guideline for all the state institutions to work in a coordinated manner. Without adopting such policy level thinking, the results would be unsustainable, short-term and reactionary while the advantage of the preemptive strike would always remain with the terrorists and other criminals [19].

Best line of action for implementing a smart city project is to follow a framework model with clear horizontal and vertical coordination through well-contemplated procedures and protocols. The framework must address exceptional scenarios as well.

A coordinated framework at a policy level can be developed only if all coordinated bodies demonstrate a leadership role during this process. Institutional leadership must be able to complete strategic and critical appraisal of this framework in order to address any functional discrepancies in it. Producing such leadership at top of every institute is yet another challenge in developing nations like Pakistan where political intervention in almost every state institution has compromised its quality of leadership.

The framework must guide how to interact with different departments in a ministry or which protocol to follow when asking for assistance to another ministry. Similarly, it must provide means to include the non-state actors like NGOs and community members for their input and suggestions.

Such frameworks are hard to cite in developing nations and it is their absence which is one of the core reasons for developing nations to be such. The absence of integrated coordinated framework leads to waste of resources and contradictory policymaking. Pakistan is a prime example in many departments.

B. Governance Level

Grander stress on security as a public good improves the need for teamwork and corporations of customary and non-traditional players in the development of a smart city project framework. A broad-based methodology to build consent on such a framework leads to the process of founding indigenous alliances and trusts based on the idea of co-producing a safe environment for all.

City government and departments have a role to play in enabling such working alliances while the resources must come from federal and provincial governments along with national and provincial level policy guidelines.

It is also critical to map early the potential stakeholders which can play a role in the implementation of a smart city project at any stage. This helps in presenting the idea to that particular stakeholder with the clearly defined role of that stakeholder in it. This gives an added sense of purpose and responsibility hence enhances the level of social inclusion. This is also a crucial step because it allows the nonstate actors to align their policy and strategic planning with public institutions which in the long run will help them by making the execution of their own program smoother [20].

Many cities, principally faced with high crime rates have effectively undertaken the elimination of urban crimes, violence, and insecurity by turning it into an opportunity for new citizens' engagements. These success stories have highlighted that good governance and smart cities are reciprocal variables. Better the level of governance lower the probability of violent incidents and instability in the city.

C. Technical Level

The biggest challenge in implementing a secure city project stems from the fact that it must be able to secure the information gathered at the sensory layer of the system through CCTVs and other means. Information about the privacy of the individuals is particularly sensitive and must be secured at all costs [21].

Availability of a strong communication infrastructure is another big technical challenge to the smart city initiative. Cities with fiber optic connectivity and the presence of well-established Wi-Fi and other wireless technologies are more suitable candidates for a smart city project than those where such communication technologies are not available [22]. Though these can be established at any stage in developing countries finding the necessary political will to accomplish such pre requisites become a challenge in itself.

Availability of trained human resource to handle all the devices, communication networks, storage facilities, network management and security following the guidelines set in the policy-level framework is also among the most critical requirements for a smart city project to be completed successfully.

D. Financial Level

Finances are an obvious challenge for the physical implementation of such a complex and advanced concept in a large city. The financial the constraint may eventually lead to compromise some of the features intended in a smart city plan [21]. For example, the scope of a smart city the project may initially contain the provision of machine learning and Big Data services but while implementing the solution the prohibitive cost may limit the scope of the project to basic surveillance set up without any advanced features like deep learning and training neural networks for optimizing response in the future.

Financial challenge is more critical and real in the developing states and maturing cities. International assistance from financial institutions like the World Bank or the Asian Development Bank (ADB) may come handy and must be acquired because no cost is greater than human lives.

But the best strategy would be to draw private sector investment in the city so that tax money can help build such an expensive system within the available resources. The project can be implemented in phases in order to keep the per year cost of installation within the limit [6]. This may turn the project into a long-term undertaking but this implementation strategy would not constrain the available resources with the city administration. Areas for implementing the security system can be prioritized based on requirements or perceived threat levels.

VII. Conclusion

Smart cities require dozens and in some cases, hundreds of small and large-scale initiatives at a different level in different institutions in the cities to be able to emerge on a responsive security framework. One such example of multiple initiatives is Safe Dubai project. An ambitious city safety project was undertaken by the UAE government where billions of small or large IP based devices would be generating the considerably higher amount of data to be processed and analyzed. It is estimated that during the course of its implementation till 2020, the project will connect more than 20 billion smart devices through IoT networks. This massive network will provide the input for information processing units which will be running mainly on PoE. This advanced project is only of a kind in the world and it will usher a new era in smart city planning.

References

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] F. Mosannenzadeh, A. Bisello, R. Vaccaro, V. D'Alonzo, G. W. Hunter, and D. Vettorato, "Smart energy city development: A story told by urban planners," *Cities*, vol. 64, pp. 54–65, 2017.

[3] F. Jameel, "Network security challenges in smart grid," in *2016 19th International Multi-Topic Conference (INMIC)*. IEEE, 2016, pp. 1–7.

[4] M. Yasuoka, "Designing a safe city eco system for wandering," in *Dementia*, 2017.

[5] A. Cocchia, "Smart and digital city: A systematic literature review," in *Smart city*. Springer, 2014, pp. 13–43.

[6] Z. Allam and P. Newman, "Redefining the smart city: Culture, metabolism and governance," *Smart Cities*, vol. 1, no. 1, pp. 4–25, 2018.

[7] E. E. Joh, "Policing the smart city," 2018.

[8] O. E. G. Bates and A. J. Friday, "Beyond data in the smart city: learning from a case study of re-purposing existing campus iot," *IEEE Pervasive Computing*, vol. 16, no. 2, pp. 54–60, 2017.

[9] F. Jameel, M. A. A. Haider, A. A. Butt *et al.*, "High snr analysis of inter-body interference in body area networks," in *2017 International Conference on Communication, Computing and Digital Systems (C-CODE)*. IEEE, 2017, pp. 117–121.

[10] ——, "Robust localization in wireless sensor networks using rssi," in *2017 13th International Conference on Emerging Technologies (ICET)*. IEEE, 2017, pp. 1–6.

[11] F. Jameel, A. Ali, and R. Khan, "Optimal time switching and power splitting in swipt," in *2016 19th International Multi-Topic Conference (INMIC)*. IEEE, 2016, pp. 1–5.

[12] A. Bhati, M. Hansen, and C. M. Chan, "Energy conservation through smart homes in a smart city: A lesson for singapore households," *Energy Policy*, vol. 104, pp. 230–239, 2017.

[13] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in smart city initiatives: Some stylised facts," *Cities*, vol. 38, pp. 25–36, 2014.

[14] F. Jameel, M. A. A. Haider, A. A. Butt *et al.*, "A technical review of simultaneous wireless information and power transfer (swipt)," in *2017 International Symposium on Recent Advances in Electrical Engineering (RAEE)*. IEEE, 2017, pp. 1–6.

[15] ——, "Performance analysis of vanets under rayleigh, rician, nakagami-m and weibull fading," in *2017 International Conference on Communication, Computing and Digital Systems (C-CODE)*. IEEE, 2017, pp. 127–132.

[16] P. V. Paul and R. Saraswathi, "The internet of thingsa comprehensive survey," in *Computation of Power, Energy Information and Commuincation (ICCPEIC), 2017 International Conference on*. IEEE, 2017, pp. 421–426.

[17] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, "An information framework for creating a smart city through internet of things," *IEEE Internet of Things journal*, vol. 1, no. 2, pp. 112–121, 2014.

[18] M. Yar, "E-crime 2.0: the criminological landscape of new social media," *Information & Communications Technology Law*, vol. 21, no. 3, pp. 207–219, 2012.

[19] T. Shelton, M. Zook, and A. Wiig, "The actually existing smart city," *Cambridge Journal of Regions, Economy and Society*, vol. 8, no. 1, pp. 13–25, 2015.

[20] R. G. Hollands, "Critical interventions into the corporate smart city," *Cambridge Journal of Regions, Economy and Society*, vol. 8, no. 1, pp. 61–77, 2015.

[21] D. Eckhoff and I. Wagner, "Privacy in the smart cityapplications, technologies, challenges, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 489–516, 2017.

[22] V. A. Memos, K. E. Psannis, Y. Ishibashi, B.-G. Kim, and B. B. Gupta, "An efficient algorithm for media-based surveillance system (eamsus) in iot smart city framework," *Future Generation Computer Systems*, vol. 83, pp. 619–628, 2018.