IJCCN | INTERNATIONAL JOURNAL OF COMPUTING & COMMUNICATION NETWORKS

ISSN: 2664-9519 (Online); Vol. 1, Issue 2, November 2019

Cyber Physical System based Crime Resistant Model for Smart Cities

Sundus Qayyum and Ayesha Naveed

Department of Computer Science, Bahria University Islamabad, Pakistan

* Corresponding Author: qayyum.sundas@gmail.com

Received; 25 September, Revised; 5 November; Accepted; 20 November

Abstract: The technology development, as well as its improvement, has been growing rapidly with every passing day. One of the emerging areas is the Internet of Things (IoT) based on new information and communication-based technologies and Cyber-Physical Systems (CPS). The IoT and CPS can be integrated into various domains in smart cities like energy, automation, industries, smart cities, smart homes. In context to the smart city applications, the smart cities must be safe and secure models and provide a safe and secure crime-free resistant city. Using this aim in this paper, we propose a conceptual model for smart cities. This model presents the two modules including Smart Vehicle & Human Safety (SVHS) and Safe Streets Model (SSM). These modules help the victims in case of any emergency and provide a more secure and safe environment.

Keywords: *IoT, CPS, Safe city, Street Crime, Security, Smart*

1. Introduction

The population density increases in urban areas rapidly; simultaneously the demand in supporting structures and the services are also increased to meet the requirement of people. Citizens need a safe, secure and quality lifestyle. In delivering these demands, we have to face social and economic development challenges. Then the concept of smart cities came. Smart cities can be defined as installation of intelligent digital ecosystems in the urban areas which focused on improving urban lifestyle in six domains: people, government, economy, mobility, environment and living [1, 2]. Smart cities have been set up using advanced Information and Communication Technology (ICT) infrastructures such as Internet of Things (IoT) [3].

IoT is the integration of internet with physical things or objects. Those physical objects can be home appliances, vehicles and smart phones. The key elements of IoT are the sensors and actuators. IoT devices eliminate the dependency on human for the data creation, processing, analyzing and taking the action against. However, talking about the application development for IoT could be a challenging task because of the difficulty level, lack of policies, various programming languages protocols [4, 5]. Besides providing ease to users, the wireless network components of IoT are at high risk because of their vulnerabilities. These wireless networks are a part of critical infrastructures like military, business, healthcare, retail, and transportations. So its protection is must [6]. A Cyber Physical System (CPS) incorporates the safe, secure and efficient data communication, computation and information storage of physical objects with simultaneous controlling and monitoring of the systems in a real-time [7, 8]. The combine applications of IoT and CPS include smart cities, smart homes, healthcare, transport, agriculture, smart supply chain, smart grids, environment, real-time location, occupancy of parking spaces, traffic jams etc., Figure 1 shows the integration of IoT and CPS. All these applications are used to facilitate the human in quick and easy manner.

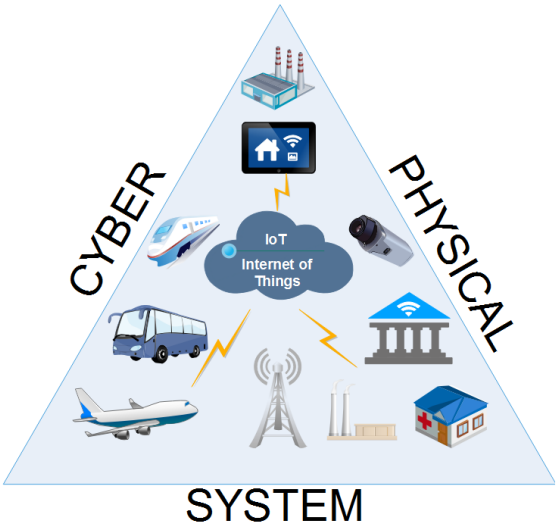

Figure 1. Applications of CPS and IoT

Now a day, street crimes like robbing, car snatching and kidnapping have been increased. These street crimes not only affect the people financially but also morally. Science and technology has to play its role in controlling these types of crimes. For this the National Crime Prevention Institute takes an initiative of a certified crime prevention community program with the name the Crime Prevention Through Environmental Design (CPTED) which states that:

> *"The proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, and an improvement of the quality of life."*

CPTED has four working strategies as shown in Figure 2. According to CPTED, there is a relationship between the build environment and criminal behavior. The strategies explained in CPTED provides guidelines for the professional designers, developers or remodelers to reduce occurrence risk of crime [9].

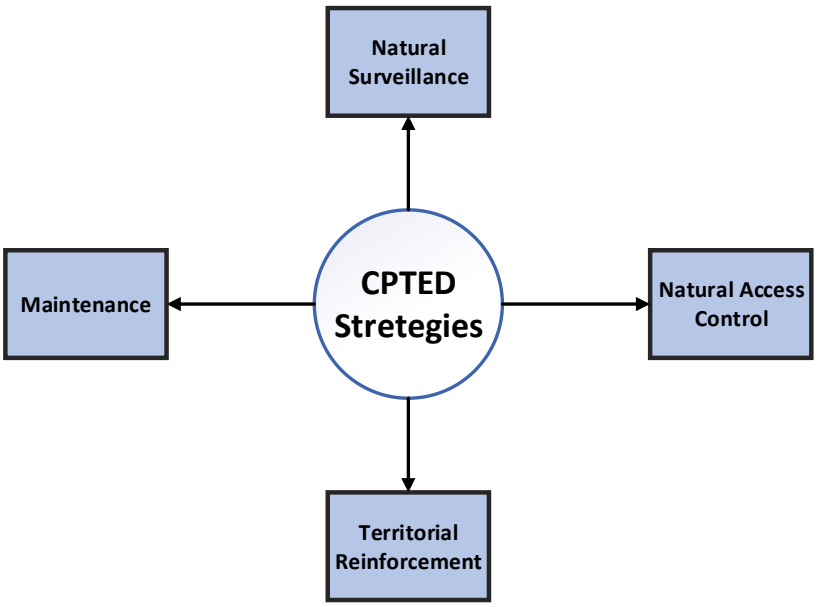

Figure 2. CPTED Strategies

This paper proposes a two frameworks called Smart Vehicle & Human Safety (SVHS) device and Safe Street Model (SSM) for smart cities. The basic concept behind the proposed model is securing the vehicles safety from snatching. Whereas in SSM, the basic idea behind is making the smart cities free from streets crimes like mobile snatching, kidnapping and harassing.

The rest of paper is organized as follows: Section 2 provides the related work in the area of smart cities. Section 3 presents the proposed model design and development phases. Section 4 discusses the physical model of proposed model. The paper concludes in last section with future direction.

2. Related work

Several papers regarding the concept of safe cities have been published. One of them is described in [10] in which a prototype application named SVS (Social Video Streaming) is designed to stop the street crimes. This application is android based and uses Wi-Fi for the live streaming of the event. The protocol RTSP (Real-Time Streaming Protocol) is used for live monitoring which sends the live packet to recording the server RTSP to assists the police department to get alert for any incident that happens. In addition, to live video sharing, recorded videos of incidents can also be sent to police officers. SVS can also track the incident location. The proposed prototype is at the design level and near more research for its practical implementation.

One more review paper is presented in [11] in which the survey is carried out regarding the issues faced by smart cities that are privacy and security, it also explains the current and future work in this field. The paper describes the various classifications of smart cities in terms of their structure, parts, and functions. The paper identifies the privacy and security issues by finding the gap in the architecture of smart cities. After a detailed analysis of challenges, requirements, and issues of smart city security, the author proposed the pros and cons of various available methods. And lastly, the future directions are also given for further enhancement. As we know, the smart cities are very useful for the user in terms of services, applications, convenience but along with these benefits, there are also some loopholes present in these services. Among those loopholes, the authentication of the data is most important.

The authors in paper [12] proposed an IoT, big data, artificial intelligence are all interlinked with the cyber-physical system. All the data is gathered from any of these sources need to be secure and authenticated. The data leakage by any means is the risk. This risk is measured using the Factor Analysis of Information Risk (FAIR) model, from different elements in the CPS environment. This model is used for situational awareness of CPS. The attack risk is reduced by Crime Prevention Through Environmental Design (CPTED). The successful simulation results of reducing risk are also shown in this paper.

For reducing the street crimes, one more approach is described in the paper [13] using drone technology. As we know that drone is used in various applications like military, agriculture, aerial photography, surveillance, remote sensing, and many more purposes. The author utilizes this approach for controlling and monitoring the street crimes. For this he split the task into two processes, in the first process' real-time monitoring is done and in the second process, its controlling, monitoring and target operations are done. The diameter range of the monitoring drone is 5km. The operator is there to control the drone movement. To detect the shape of the weapon, the algorithm is designed and tested. The matching results are also shown in the paper. Future work for the improvement of weapon detection under the shadow region will be focused.

Regarding the safety of the vehicle, the various literature articles are present. One of them proposed a prototype in [14] using IoT for smart parking management and the concept of smart vehicles and its safety. Related to our framework, vehicle safety is implemented using the fingerprints of the user and the technology integrated is RFID and IOT along with Arduino UNO with GPS, GSM and vibration motor. The other author says that smart cities are necessary for securing the cities from street crimes. The main objective of this paper [15] is exploring all possible digital ways in avoidance of street crimes. The author gathered the crime data for all days of the week from the Academy of Management of the Ministry of Internal Affairs of the Russian Federation from 2009-2011 and 2015-2017. As a result of this data, the two approaches are defined for the prevention purpose. One is to highlight the streets according to their criminal rate level. Secondly, the safety purpose boards must be paste on the street walls which will help the victim in handling emergencies.

Table 1. Comparison of Literature Data

Ref#	Method Name	Type	
		Framework Based	Literature Based
[16]	SVS	√	×
[17]	Review Based	×	√
[12]	FAIR	√	×
[18]	Drone Based	√	×
[19]	IoT + RFID	√	×
[20]	Data Analysis Based	×	√

3. Proposed Model

In this section, we introduce the two module for smart cities framework including Smart Vehicle & Human Safety (SVHS) and Safe Streets Model (SSM).

3.1 Module-I

The first module is SVHS, where the conceptual security model for car snatching along with emergency situation handling is proposed. According to the concept, firstly the user needs to get registered for his car and get the device. The device is already installed in the car. The function of the device is to share a live user location and detect the weapon around the car. In case of any emergency, the device will generate an alarm at the monitoring cell.

Consider the case I: in which the user gets an emergency, the user may push the emergency button. The emergency could be any type such as medical issues, road fear, and accident. After pressing the emergency stop button, the alarm generates at the monitoring cell. The monitoring team marks or locks the current location and get the recent images from the nearby cameras. Then the monitoring team will call the user at the registered number to inquire about the situation and if the user acknowledged then the alarm will be removed. In other situations, if an emergency alarm generated and the user did not respond, it means the user needs help. Then the monitoring cell instantly informed the closest emergency response team for the help of the user.

In case II: if the user is moving on the road and suddenly surrounded by some thieves having weapons along with them, then the installed smart device detects the weapon and generates the emergency alarm and the rest same actions are performed as mentioned in Figure 3.

3.2 Module-II

The module-II named SSM presents the conceptual model of kidnapping and snatching crimes in the streets. The idea starts with continuous monitoring of streets and this monitoring is completed by installing intelligent cameras inside the street. Intelligent cameras mean that they are artificially intelligent and have some built-in gestures referred to which it can compare the live stream and take decision wisely.

These cameras will also have IoT sensors installed with them. The IoT sensors will perform two tasks. One key function is live data collection from intelligent cameras and secondly, live data transmission to monitoring cells. It is proposed that continuous monitoring is carried out by the intelligent cameras and when some sort of snatching or kidnapping gestures is monitored by the cameras an emergency notification is prompt at monitoring cell.

In the monitoring room, the supervisor team will immediately watch the location where the alarm is being generated. In response to this emergency situation, the monitoring team will instantly inform the police station for the help of the victim. In case, this emergency situation is overlooked by the monitoring staff, an automatic notification will be generated by the monitoring system and send it to the concerned police station. The basic flow chart of this concept is shown in Figure 4.

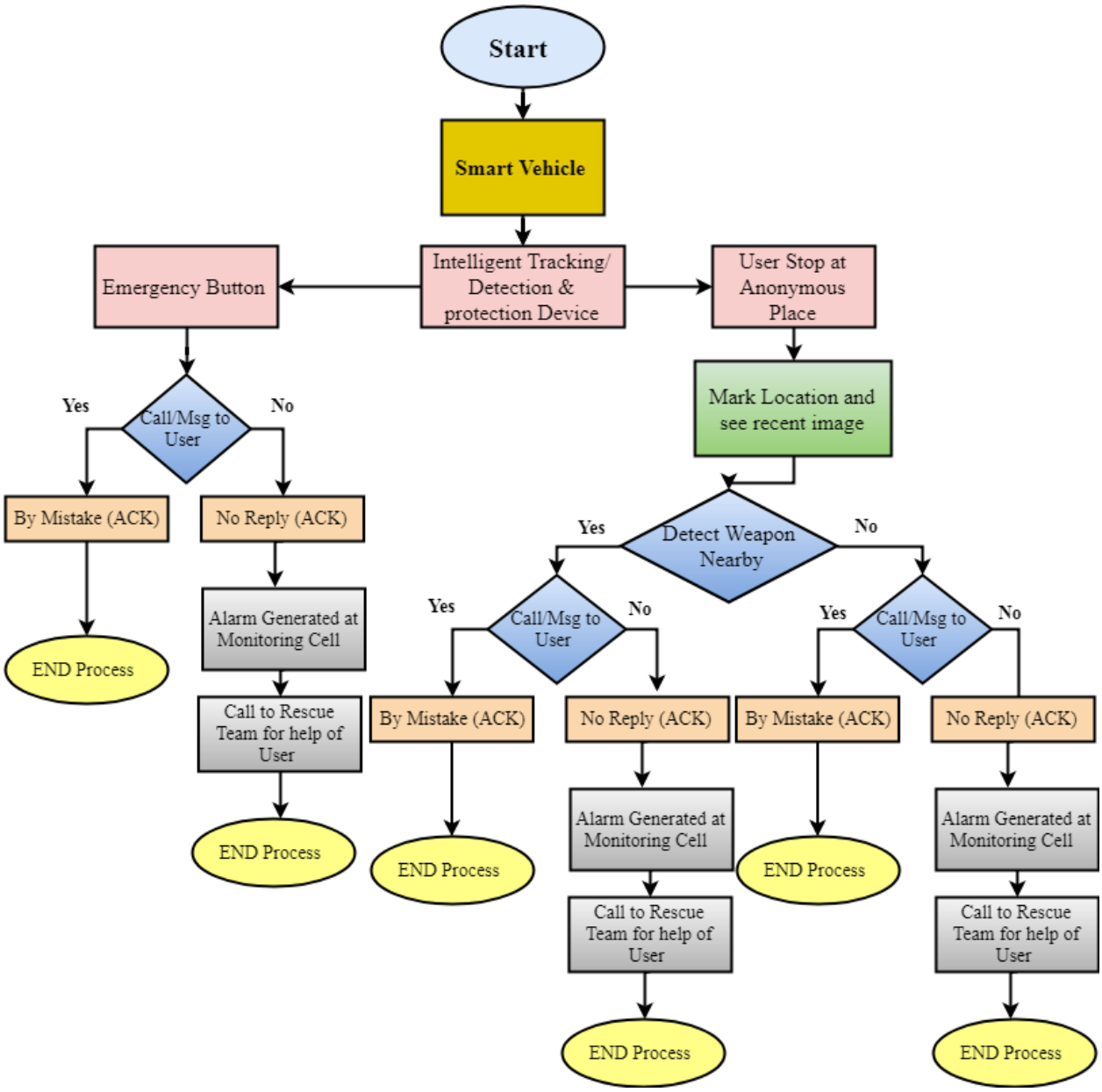

Figure 3. Flow chart of SVHS

Now as far as the security is concerned, the CPS will work for this. This means the physical process generates the live data and that data must be protected from being an intrusion, tampering, modification, etc.

The real-time data needs to be protected. This protection will be done by encrypting the data before transmission and decrypting it before displaying it in the monitoring cell.

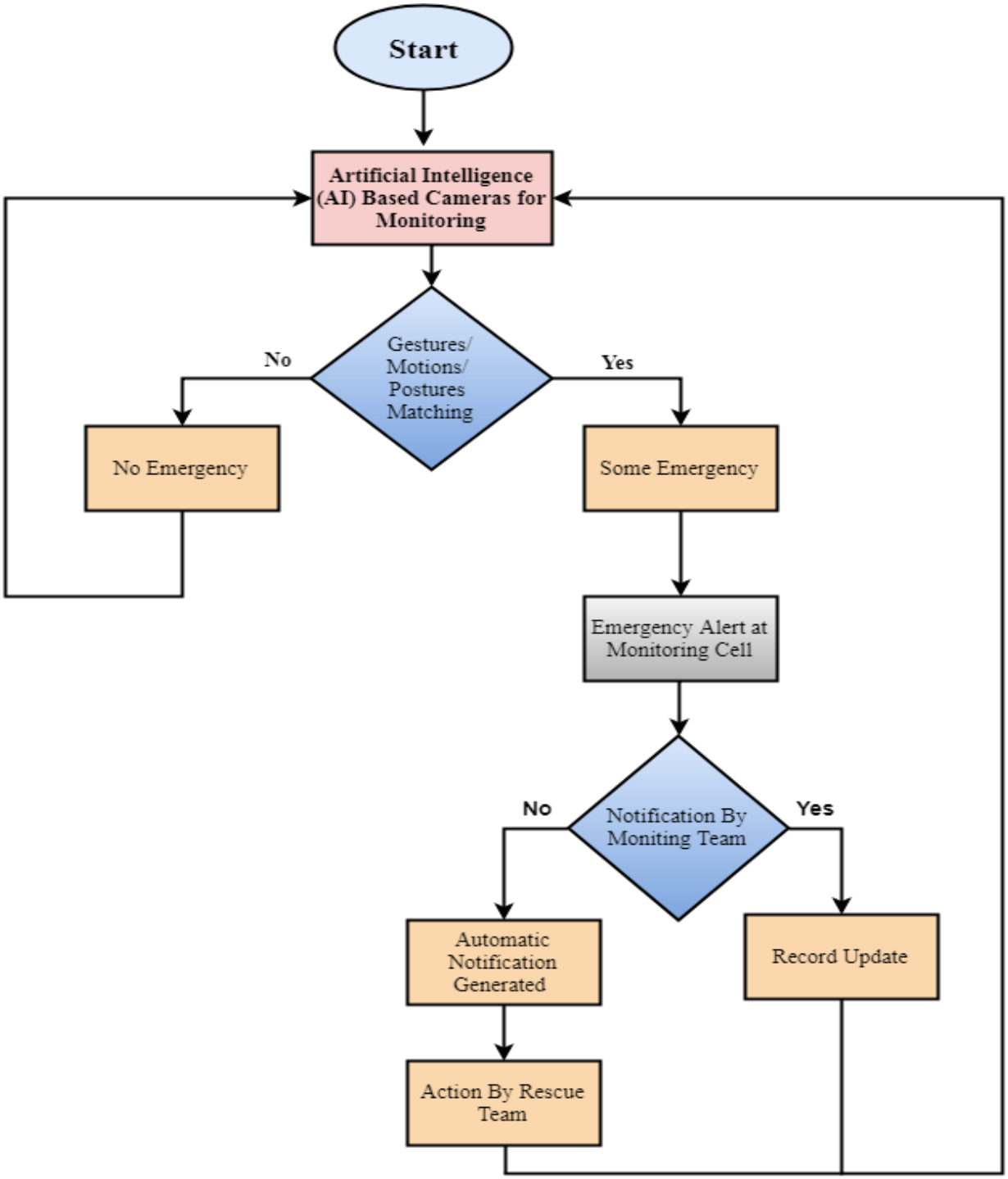

Figure 4. Flow chart of SSM

4. Physical Model of Proposed Framework

The physical model of the proposed framework is shown in Figure 5. In this physical model, the locations marked with dotted circles where the data monitored, gathered, analyzed and then action will be performed at different ways. The blue circles show the wireless connectivity at different locations with IoT. Table 2 shows the different standards used in proposed framework.

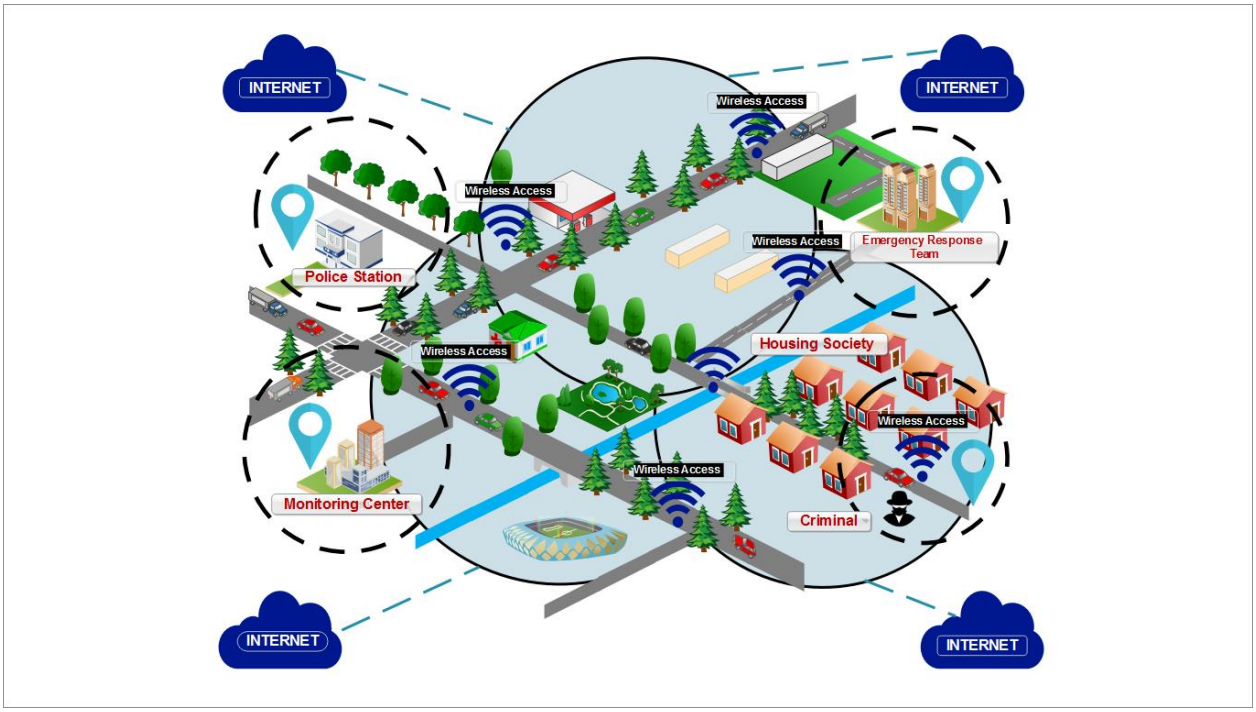

Figure 5. Physical Model of Proposed Concept

Table 2: Standards for data communication

Ref#	Technology	Standards	
[21]	CPS	NIST SP 1500-201	
[22, 23]	IoT	Application Layer:	CoAP
		Network Layer:	6LoWPAN
		Data Link Layer:	IEEE 802.15.4
[24]	Environmental Monitoring	CPTED	

5. Conclusion

In this paper, we proposed a smart city framework called Vehicle & Human Safety (SVHS) device and Safe Street Model (SSM). In the SVHS model, the concept of Vehicle safety from snatching is addressed. Whereas in SSM, the idea is to make safe and crime-free streets especially for mobile snatching, kidnapping and harassing cases. The framework provides more efficient decisions at the emergency and new and integrated technologies provide more comfort to users. The technology we used is IoT, CPS and AI-based cameras for detection and monitoring purposes. In future work, we use AI cameras for the detection of wanted criminals. This will help law enforcement agencies to trap criminals.

References

[1] L. Anthopoulos, M. Janssen, and V. Weerakkody, "A Unified Smart City Model (USCM) for smart city conceptualization and benchmarking," in *Smart Cities and Smart Spaces: Concepts, Methodologies, Tools, and Applications*: IGI Global, 2019, pp. 247-264.

[2] K. N. Qureshi, M. M. Idrees, J. Lloret, and I. Bosch, "Self-Assessment Based Clustering Data Dissemination for Sparse and Dense Traffic Conditions for Internet of Vehicles," *IEEE Access*, vol. 8, pp. 10363-10372, 2020.

[3] V. Scuotto, A. Ferraris, and S. Bresciani, "Internet of Things: applications and challenges in smart cities. A case study of IBM smart city projects," *Business Process Management Journal*, 2016.

[4] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *Journal of Information Security Applications,* vol. 38, pp. 8-27, 2018.

[5] K. N. Qureshi, F. Bashir, and A. H. Abdullah, "Provision of Security in Vehicular Ad hoc Networks through An Intelligent Secure Routing Scheme," in *2017 International Conference on Frontiers of Information Technology (FIT)*, 2017, pp. 200-205: IEEE.

[6] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, "Security issues in the Internet of Things (IoT): a comprehensive study," *International Journal of Advanced Computer Science Applications,* vol. 8, no. 6, pp. 383-388, 2017.

[7] J. Wurm *et al.*, "Introduction to cyber-physical system security: A cross-layer perspective," vol. 3, no. 3, pp. 215-227, 2016.

[8] K. N. Qureshi, F. Bashir, and N. U. Islam, "Link Aware High Data Transmission Approach for Internet of Vehicles," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1-5: IEEE.

[9] J. H. J. P. p. Ratcliffe and research, "The hotspot matrix: A framework for the spatio-temporal targeting of crime reduction," vol. 5, no. 1, pp. 5-23, 2004.

[10] Z. Bhutto, K. Dahri, I. Lakho, and S. Memon, "Social Video Streaming (SVS): A prototype application for street crime reporting," in *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2015, pp. 1-4: IEEE.

[11] M. Sookhak, H. Tang, Y. He, F. R. J. I. C. S. Yu, and Tutorials, "Security and privacy of smart cities: a survey, research issues and challenges," vol. 21, no. 2, pp. 1718-1743, 2018.

[12] M. Joo, J. Seo, J. Oh, M. Park, and K. Lee, "Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System," in *2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2018, pp. 837-842: IEEE.

[13] S. Karim, Y. Zhang, A. A. Laghari, and M. R. Asif, "Image processing based proposed drone for detecting and controlling street crimes," in *2017 IEEE 17th International Conference on Communication Technology (ICCT)*, 2017, pp. 1725-1730: IEEE.

[14] G. Pareek and M. Vinay, *IoT based Prototype for Smart Vehicle and Parking Management System* (2018). 2018.

[15] Y. V. Truntsevsky, I. Lukiny, A. Sumachev, and A. Kopytova, "A smart city is a safe city: the current status of street crime and its victim prevention using a digital application," in *MATEC Web of Conferences*, 2018, vol. 170, p. 01067: EDP Sciences.

[16] Z. Bhutto, K. Dahri, I. Lakho, and S. Memon, "Social Video Streaming (SVS): A prototype application for street crime reporting," in *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on*, 2015, pp. 1-4: IEEE.

[17] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues and Challenges," *IEEE Communications Surveys & Tutorials,* 2018.

[18] S. Karim, Y. Zhang, A. A. Laghari, and M. R. Asif, "Image processing based proposed drone for detecting and controlling street crimes," in *Communication Technology (ICCT), 2017 IEEE 17th International Conference on*, 2017, pp. 1725-1730: IEEE.

[19] G. Pareek and M. Vinay, "IoT based Prototype for Smart Vehicle and Parking Management System," *Indian Journal of Science and Technology,* vol. 8, no. 1, 2018.

[20] Y. Truntsevsky, I. Lukiny, A. Sumachev, and A. Kopytova, "A smart city is a safe city: the current status of street crime and its victim prevention using a digital application," in *MATEC Web of Conferences*, 2018, vol. 170, p. 01067: EDP Sciences.

[21] E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-physical systems: Volume 2, working group reports," 2017.

[22] Z. Sheng, S. Yang, Y. Yu, A. Vasilakos, J. Mccann, and K. Leung, "A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities," *IEEE Wireless Communications,* vol. 20, no. 6, pp. 91-98, 2013.

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

[24] A. N. A. L. E. AGENCY. (2004). *CPTED STRATEGIES* Available: http://www.pwcgov.org/government/dept/police/Documents/002035.pdf