Radioelectronic and Computer Systems, 2024, No. 1(109)
ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

UDC 621.397.42.038.616:004.77

DOI: 10.32620/reks.2024.1.10

Himani SHARMA, Navdeep KANWAL

Punjabi University Patiala, Punjab, India

SMART SURVEILLANCE USING IOT: A REVIEW

In today's modern society, video surveillance is a growing trend and it can revolutionize many aspects of technology, especially in future smart cities that will transform traditional surveillance systems into intelligent and interconnected networks. It may be difficult for even well-trained employees to process and respond immediately to monitored data. Moreover, IoT-enabled surveillance systems overcome the challenges and flaws of conventional passive monitoring techniques by offering real-time surveillance and automated notifications for suspicious activity, intrusions, or anomalies. Therefore, the ***objective of this*** *article is to provide an Internet of Things (IoT)-based smart surveillance system that may successfully connect the ecosystem, resulting in enhanced monitoring for smart city services. The primary* ***goal*** *of this study is to provide a comprehensive review of several IoT-based surveillance techniques used in various smart city applications. The categorization of* ***tasks*** *for each section is as follows: to present the historical context overview; to examine the significance of IoT and its application in smart cities; to present a standardized architecture for IoT-based smart city surveillance; to highlight an authoritative and thorough review of current IoT-based smart surveillance systems; and to identify various research issues. The* ***methods*** *used are: statistical graph or chart approach, schematic, and timeline diagram.* ***Conclusions.*** *This article outlines numerous research challenges for future video surveillance that may be addressed by researchers. In summary, this comprehensive review provides a valuable and streamlined resource for future researchers exploring smart city surveillance through the IoT.*

Keywords: *Smart Cities; video surveillance system; Video Forgery Detection; IoT Architecture*.

1. Introduction & Motivation

Over the past few decades, an enormous number of technological and scientific development efforts have been invested in video surveillance. It is further being enriched with Internet of Things (IoT) intelligence so that automatic or smart surveillance can be implemented. This IoT-based smart surveillance allows individuals and law enforcement agencies to better monitor specific regions by detecting anomalous events. Therefore, the need for smart surveillance has risen exponentially throughout the last decade, leading to a new Internet of Things paradigm [1]. IoT is a domain that influences not just everyday lives but also affects the way people connect with each other [2]. The key motivation behind the research in IoT-based smart surveillance is that it enables individuals to obtain rapid and trustworthy information regarding activities and artifacts present in the real world. The capability to collect information using sensors and communicate data over the internet are crucial considerations of an "IoT object" [3, 4]. Moreover, the integration of every IoT device with devices that acquire and analyze information and can transmit it through the network as per the requirement may lead to the construction of smarter cities. Internet access allows the devices to identify themselves in the network as well as to create a smart system that is crucial for communicating across different interfaces of mobility, governance, technology, and environment [5]. Consequently, both IoT and video surveillance have become essential parts of smart cities.

In modern day era, publishing research trends for "smart city", "IoT-based video surveillance", "IoT-based Smart City Surveillance" as well as "IoT in smart cities" have evolved exponentially [6]. Numerous researchers have recommended several ways to improve the smartness of a city [7]. The range of research publications in the last few years is presented in Figure 1. The chart illustrates the continuous spike in research related to smart cities over the past several decades.

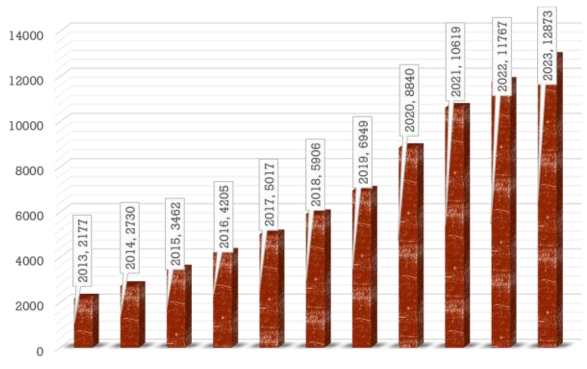

Fig. 1. "Smart Cities", "IoT in Smart Cities" and "IoT-based Smart Video Surveillance" research trend of the last 10 years

1.2. Paper Organization

The present paper concentrates on the existing scenario in the application areas of smart cities, and the current challenges and future prospects in this domain. This survey's organizational structure is presented in six sections. The structure of each section, and a discussion of all subsections, is shown in Figure 2. The primary aim of the current study is to acknowledge the challenges of prior research in this area. It focuses more specifically on the persistent issue of the video content's integrity and authenticity. The entire article is divided into the following five sections. Digital image and video surveillance are briefly explained in Section 1 along with the study's purpose and main contributions. Background information and a generic smart surveillance architecture have been described in Section 2. Additional significant publications on video surveillance for the last 10 years are reviewed in Section 3 along with a comprehensive study of their detection techniques. The applicability and gaps in the existing literature of the different IoT-based surveillance approaches are clearly and unambiguously discussed in this study. In Section 4, the nature of the problem with the suggested strategy is explained, along with its challenges and contributing factors. Section 5 concludes by summarizing the entire project and offering suggestions for further research in the field of smart video surveillance.

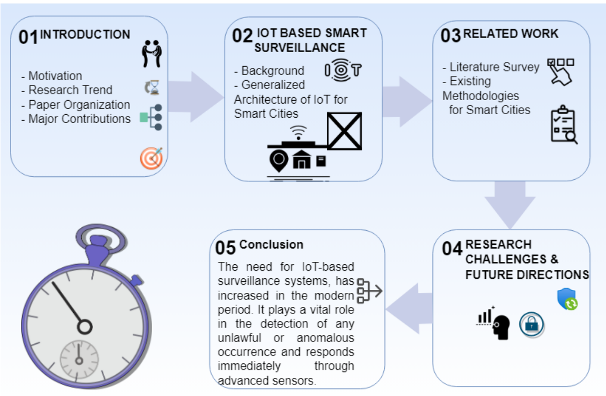

Fig. 2. Paper Organization

1.3. Major Contributions of Present Study

This study additionally presents a thorough analysis of smart cities motivated by the Internet of Things and includes the following significant contributions:

– presents an IoT-based layered architecture for a promising direction for future scholars in the field;

– provides an analysis of the techniques used to implement intelligence into IoT-based video surveillance models for smart cities;

– discussed current research challenges in IoT-based technologies for smart cities.

2. Background

Radio-frequency identification (RFID) technology & wireless sensor networks (WSN) are the key foundations of the Internet of Things (IoT) [8]. With RFID readers, individuals can immediately identify, track, and monitor all RFID-linked things. Warehousing, medical manufacturing, marketing, and supplier management are the application fields of RFID [9]. Thus, RFID, with its readers and tags, plays a critical role in IoT applications. Moreover, wireless sensor networks (WSN) make extensive use of interconnected smart sensors to enable sensing and surveillance [10, 11]. Technological advancements in RFID and WSN have simultaneously contributed toward IoT development.

Kevin Ashton originally suggested IoT in his presentation in 1999 [12]. It is a growing architecture of worldwide network-based information services, particularly for the Internet [13]. IoT therefore seeks to increase the integration and pervasiveness of the Internet. IoT was originally intended to allow communication between businesses in the world logistics system. Academicians later integrated IoT with smart inventions, which included sensing, actuation, satellite, and other advanced technologies. Core perspectives of IoT are: Things-oriented, Internet-oriented, and Semantic-oriented visions [3, 13]. Things are represented in the initial vision by their identification, and the first definition of IoT originated from the viewpoint of things-oriented vision. Second, networking, as the United Nations has recommended, is a key component of the Internet-oriented vision. In a somaticize vision, the data provided by the IoT can be modeled accordingly. IoT ambitions play a crucial role in the development of a smart city. In numerous operations in diverse contexts, IoT-based systems are feasible. Thus, it has many diverse inventions to cope with. These innovative inventions use various technologies to advance civilization. The concept 'smart city' originated in the early 1990s, and academics emphasized the process of urban development, automation, innovations, and globalization [14]. The phrase Smart Cities was initially coined as wired cities in the contemporary wireless communications technology era. However, owing to subsequent advancements, the word wired has lost its significance [15]. Figure 3 shows the consistent development of technologies and future predictions associated with the IoT across smart cities. The World Economic Forum identified the Internet of Things as one of the top three impactful technology developments, looking for its recognition of expanding significance[16].

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

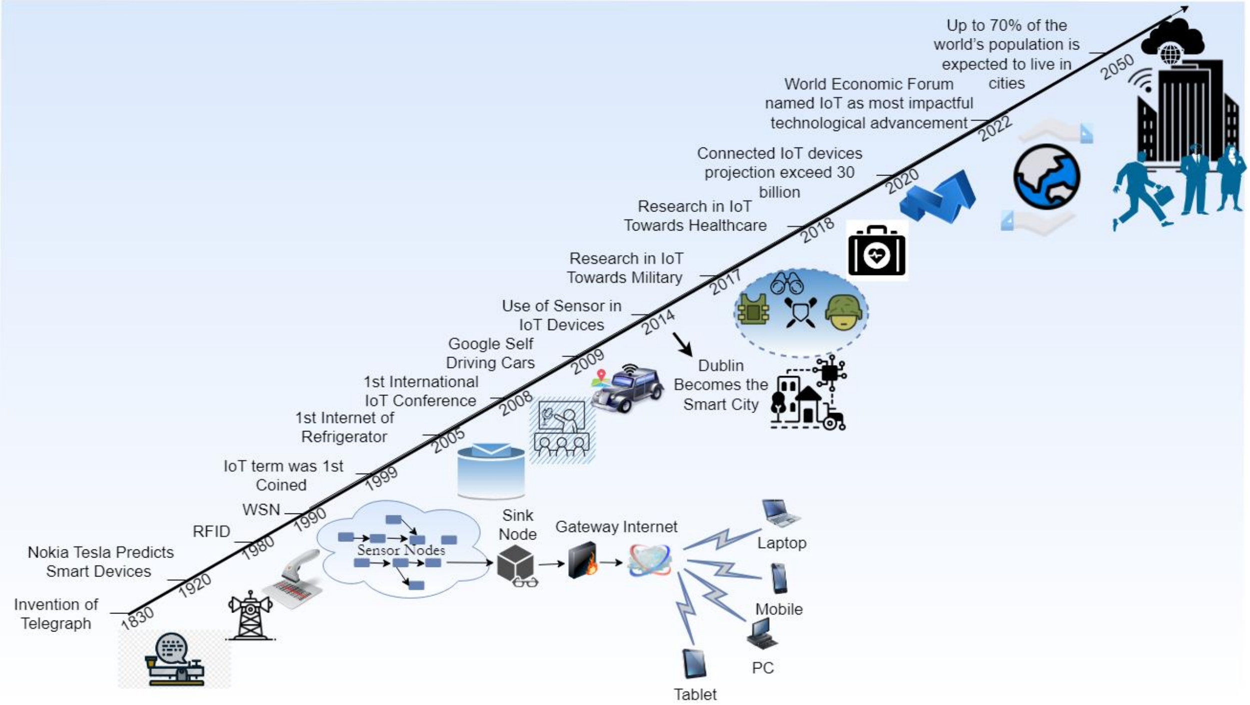

Fig. 3. Evolution of IoT in Smart Cities

2.1. Generalized Architecture of IoT for Smart Cities

Several frameworks have been developed by numerous researchers to explore the evolution of smart cities [17, 18]. IBM suggested the initial smart city architecture in [19]. The proposed hybrid IoT-based smart city architecture is shown in Figure 4. It includes layers [20, 21]: coding, perception, network, middleware, application and in the end business layer.

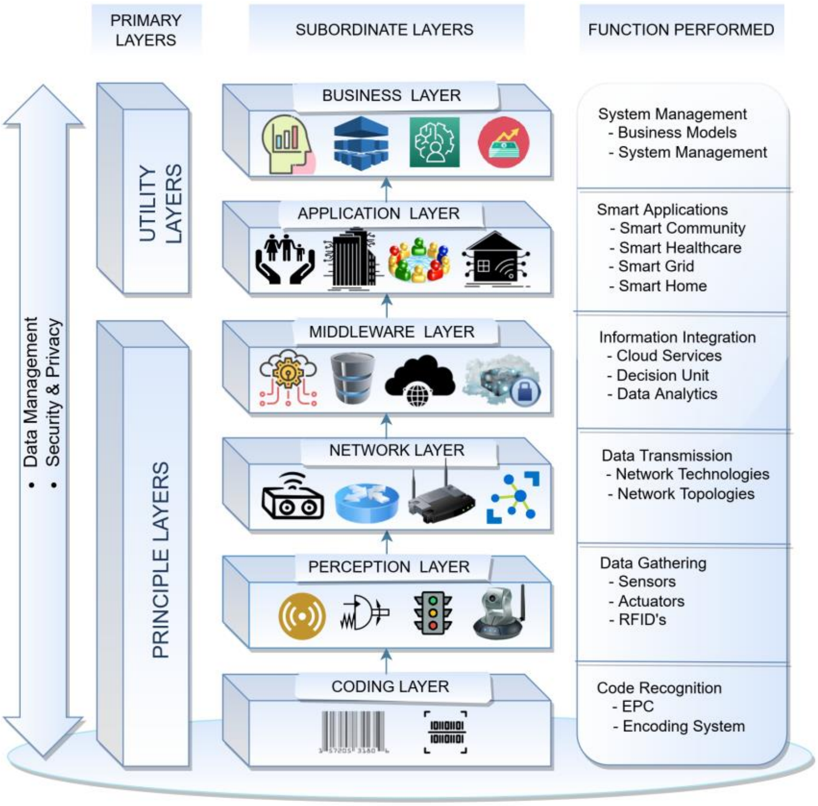

Fig. 4. Generalized Architecture of IoT for Smart Cities

The following subsections provide a concise overview of the architectural layers. The architecture describes different aspects and the functions of each layer. The following sections include a brief description of the architectural layers.

Coding Layer

The layer is most significant according to the author in [22] and is also the backbone of the IoT. The code for each item gives an identification number, so objects can be identified throughout the entire Internet cycle.

Perception Layer

This layer is sometimes pronounced as a sensing layer. Data gathering is the core objective of this layer. It contains several types of physical devices that utilize sensors for acquiring real-time information and thus respond using actuators. A system or equipment can be linked to several sensors to gather distinct information. This layer collects data from the associated item and communicates it to the next network (higher) layer for additional processing.

Network Layer

The network layer also functions as the transport layer. The fundamental goal of this layer is the secure transfer of information between the sensory layer and the middleware layer. In addition, all network devices (switch, firewall, bridge, hub and router) are included in this network layer [23]. Reliable data transmission is also the responsibility of all devices. More specifically, it links all IoT infrastructure nodes and creates a smart platform. It also offers basic network support and data transmission through wired or wireless networks. It establishes a data routing path so that data packets may be sent to the middleware layer over the network for additional processing.

Middleware Layer

The core functionality of middleware layer is information integration. A general pipeline for the perception layer hardware and the application layer is provided by the middleware layer. This layer provides access services to consumers through various APIs and database management services. Moreover, in this layer, technological advancements such as cloud, fog, edge computing etc. are utilized, to make it easy to store and obtain relevant information in real time [2, 12, 24].

Application Layer

The key motive of the layer is to provide individualized services based on the customer or user's request and the processed data. It is responsible for deploying various applications under various circumstances. Furthermore, it is used to manage and process middleware layer data and delivers smart services to users [25]. The subsequent sections provide a more detailed explanation of each application.

Business Layer

This is the uppermost layer, which is also responsible for system administration. This layer collects all service and IoT infrastructure data and represents it with business models and visualizations (smart chart, graphs, etc). This layer analyzes the output of each of the previously described levels to improve services and preserve data confidentiality. Administrators can use this analyzed information to contribute and manage an IoT system's surveillance, analytics, deployment, review, and other advancements. As a result, the higher business layer is linked to the lower (application) layer and further establishes rules and regulations to assist the overall management of the system.

3. Related Works

Due to the built-in processing power of everyday objects, the IoT has entered a modern age of belongingness involving devices such as computers, sensors, telephones, automobiles, and useful appliances [26, 27]. Because the paradigm has shifted, it is possible to network "anything" without needing to follow rigid channels. This section provides a detailed analysis of relevant surveys and state-of-the-art methodologies. Although researchers have made significant contributions to video surveillance in smart cities. However, there are limitations in the current research that need attention. The author [28, 29] conducted a survey on video surveillance systems in smart cities, but it lacked an exploration of IoT-based surveillance studies. Another study [30, 31] focused on IoT-based surveillance in a smart campus, neglecting broader smart city applications. Moreover, the existing review studies lack a generalized architecture, which is a fundamental component for smart surveillance system development. Therefore, the primary goal of this paper is to explore smart cities, smart video surveillance, and the usage of IoT in various applications. It further discusses the strengths and limitations of previous research in these interrelated domains. Table 1 provides a comparative overview of existing IoT-based smart city surveillance techniques.

The author [32] presented a network with densely deployed PIR sensors. These sensors provide suitable information to the main node regarding motion detection, which turns on the camera in response to the information from the PIR sensor and the energy from the camera.

In [50], the authors provide a similar plan in which they deploy a voice-assistant and camera system for emergencies in a smart home scenario.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Table 1

Comparative Overview of Existing IoT-based Smart City Surveillance Techniques

Sr. No.	Author	Year	Technology	Application	Issue Addressed & Open Challenges
1.	Jelivcic *et al.* [32]	2010	Wireless sensornet-works.	Sensor based motion detection.	This prototype achieves higher power consumption than the previous one.
2.	Saraceni *et al.* [33]	2012	LBP algorithm, OpenCV.	Sensor based motion detection.	Suggested a portable sensor for an active surveillance system that could track faces in real time.
3.	Mekonnen *et al.* [34]	2017	Wireless Multimedia Sensor Networks, (RPi).	Sensor based motion detection.	– following the appropriate protocol for a thorough shutdown of the RPi reduces power consumption; – unable to use HD videos.
4.	Mekonnen *et al.* [35]	2017	Wireless multimedia Sensor Networks.	Sensor based motion detection.	– with this, the sleepy CAM power management system for HD movies has been implemented in practice; – for an event driven surveillance application that streams full HD (1080p) video over a Wi-Fi network.
5.	Nath *et al.* [36]	2017	Patient Localization - HCSR04 ultrasonic sensor & vocal interface by Amazon Echo.	Indoor Location Detection System for Smart Home Environment.	By adding a voice-activated capability, this system will ease the transition of family members and caregivers to new technology, thereby enhancing their quality of life.
6.	Gallo *et al.* [37]	2018	Blockchain.	IoT-based Video Surveillance.	– it makes it possible to store metadata as multichain streams; – also reevaluate what immutable data from information transactions means.
7.	Mao *et al.* [38]	2019	Deep Learning in Security Framework for the IoT.	Face Occlusion Recognition.	– identifies certain criminal activities; – unable to identify faces of all ages, genders, and ethnicities. Africa, Europe, and the West are the few examples.
8.	Zamil *et al.* [39]	2019	Multilayer perceptron.	Multimedia-oriented action recognition.	– achieves high performance; – smaller area of AUC.
9.	Roque *et al.* [40]	2020	LPWAN.	LPWAN Based IoT Surveillance Systemfor Outdoor Fire Detection.	Emphasis on the precision of gas and temperature measurements during the early stages of fire.
10.	Desnanjaya *et al.* [41]	2021	IoT-based Rasp-berry Pi.	Home security monitoring system.	Keeps an eye out for undesirable occurrences such as theft, intruders, or criminals, and has plans to issue an early warning in the case of a fire, gas leak, or theft.
11.	Ravikumar *et al.* [42]	2021	ESP32 cameras.	IoT-based home monitoring system with secure data storage.	– provides consistency and secure data storage; – strict encryption using a keccak and chaotic sequence for data security; – satisfactory results are obtained.

Continuation of Table 1

Sr. No.	Author	Year	Technology	Application	Issue Addressed & Open Challenges
12.	Suhaimi *et al.* [43]	2021	NodeMCU ESP32 as amicrocontroller.	IoT-based Smart Agriculture Monitoring, Automation and Intrusion Detection System.	– android application allows farmers to actively monitor & control the irrigation operation; – users have the option of unilaterally triggering a siren to warn off any possible malicious individuals.
13.	Kumar *et al.* [44]	2021	Local binary pat tern, Raspberry Pi.	Real time visual recognition for smart city surveillance.	– for all standard databases, the lowest error rate is attained with the greatest feature reduction in the shortest amount of time; – performs well for both texture and facial recognition; – less complicated computations.
14.	Altowaijri *et al.* [45]	2021	CNN.	Cloud-based fire detection surveillance system.	– by passing attributes derived from the video acquired by the IoT device to a cloud-based service rather than the actual footage, the suggested method utilizes the cloud for fire identification; – achieved 97.5% classification accuracy.
15.	Safi *et al.* [46]	2022	LoRaWAN.	Fault Tolerant Fire Detection Surveillance System.	It can detect smoke, gas, Liquefied Petroleum Gas (LPG), propane, methane, hydrogen, alcohol, temperature, and humidity.
16.	Rajvel *et al.* [47]	2022	Edge computing& CNN.	Cloud-based System for Tracking Objects and Behavior Identification System.	– both reaction time and network bandwidth are reduced; – increases the accuracy of fall behavior prediction.
17.	Islam *et al.* [48]	2023	2D-CNN and ESN.	Anomaly Detection System for Large Video Data	– the framework suggested is compact and can be applied across edge devices to assure their viability and usefulness for IoT systems in smart cities; – limited accuracy for lower resolution dataset.
18.	Meddeb *et al.* [49]	2023	Raspberry-PI and IoT.	Surveillance robot for intruder detection & face recognition.	Less efficient in terms of accuracy for a lower resolution videos.

Moreover, the research in [33] suggests a mobile Sensor based real-time surveillance system. The d vice works independently by tracking the face of an individual who has been in the video stream for an extended period of time using an Android smartphone and a face-tracking technique. The device may also be linked to a personal computer facial recognition software via a wireless connection made possible by the smartphone.

A sleepyCAM power management system has been presented by [34] that uses a PIR sensor for the identification of motion as well as a relay to turn-on the Raspberry Pi (RPi). In sleepyCAM, the RPi is typically turned off, & a procedure for a proper shutdown of the RPi results in reduced power usage while the surveillance programme is waiting. Another author [35] built the sleepyCAM power management method for high defini-

 ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

tion movies using the Libelium Waspmote sensor platform because of preceding work [34] does not handle high definition videos. Both the RPi and Waspmote's power usage were measured using the monsoon power monitor utility. An Amazon Echo voice assistant and an ultrasonic sensor were used by the authors of [36] to locate elderly individuals in a smart home setting. Incorporating voice-based features makes it easier for family members and caretakers to acquire modern technology, enhancing the overall quality of life. For instance, [37] tracks of the location, zoom level, and viewing direction of CCTV in a smart surveillance city. The solutions contribute solely from computer vision analysis of the video stream using machine learning. An IoT framework face occlusion recognition system has been suggested by [38]. For security reasons, this effort recognizes human faces. The goal of the project is to identify human faces, and feature extraction is performed using Convolutional Neural Network (CNN) models. The authors defined a sparse classification model that can successfully identify faces. In the study [39], a method for employing Deep Learning (DL) technology to identify activities produced by IoT sensors in smart city surveillance and audio-based datasets has been presented. In addition, the research concentrated on suggesting a topological framework for multilayer neural networks. Using sensors and a Low Power Wide Area Network (LPWAN), the authors in [40] suggest a framework for outdoor fire detection. The precision of temperature and gas readings, and the prompt detection of fire, are the authors' main concerns. Another system for monitoring home security was developed by the author using a Raspberry Pi as the system's control hub [41]. The system continuously monitors home security against intruders or criminals, and even sends temperature alerts and detects smoke or gas. Additionally, [42] created a home monitoring system based on IoT that uses two ESP32 cameras for video sensing. Cloud data storage is protected and made available to enable secure storage to avoid leaking data and to preserve consistency. A rigid encryption technique using keccak and chaotic sequence has also been implemented. Another similar effort by the author [43] aims to create an intelligent monitoring and automated irrigation system to enable real-time environmental monitoring and ensure efficient irrigation usage based on specific conditions. This technique also minimizes the possibility of plant theft and prevents plant damage. The model employs a NodeMCU ESP32 microcontroller to gather environmental data using sensors, including humidity, temperature, & soil moisture levels. Farmers will be informed once the current conditions are automatically captured and detected by an ESP32 camera. To avoid open burning, warnings are also issued to farmers when unfavorable conditions, such as severe temperatures, are detected. IoT-based smart city surveillance systems using an effective rapid subspace decomposition with Chi Square transformation is suggested in a publication by [44]. A local binary pattern histogram is employed to retrieve the features for visual recognition. Fast subspace decomposition is a key factor in the memory and processing time requirements for battery-powered surveillance systems because it eliminates duplicate features. Subsequently, a method [45] using CNN and binary video descriptors is used to automatically identify fire. A related study [46] recommended implementing a surveillance system that effectively detects and prevents fires in smart buildings. By using LoRaWAN technology, this system would significantly decrease turnaround times and latency. A reliable video surveillance system must be built with fast data analytics and responsive equipment placed in a real-time cloud environment. Consequently, the Cloud-based Object Tracking and Behavior Identification System (COTBIS) was created in the study [47], and it has the ability to integrate the edge computing capabilities framework at the gateway level.

4. Existing Research Challenges & Future Directions

Many obstacles must be overcome by surveillance systems, including but not limited to infrastructural and technological issues. Thus, to offer more durable and dependable services, surveillance systems must address the following major challenges:

– to achieve IoT-based smart video surveillance, techniques that are more precise are expected, particularly in the area of behavioral analysis and anomalous activity identification;

– the challenges that surveillance systems confront today, consequently, include identification of vehicle road accidents, prediction of terrorist attacks, and multifunctional action recognition. Because they involve sophisticated computations and non-linear models, these events require much more efficient computational resources;

– the application has a significant impact on the difficulty of identifying an object of interest. People, for instance, are interested in video surveillance applications, but they are useless in traffic monitoring applications on roadways;

– digital recording sensors can record HD and HDR video, which helps the event classification model and, to a certain extent, combats poor lighting as well as other abnormalities. The growth of recorded information rates and, subsequently, the increase in necessary storage space are the consequences of integrating such sensors into surveillance systems;

– there is a need for the adaptation of new network and infrastructure technologies, such as cloud systems.

By combining surveillance systems with cloud infrastructures, the need for increased computing power and storage capacity might also be met. To gain more insightful information, this trend will also require the integration of various monitoring systems. New data formats, communication protocols, and query languages that have been specifically designed for surveillance will be required for this integration.

Conclusion

The IoT has integrated a new era of communication between computers, sensors, smart phones, automobiles, and assistive appliances. Multimedia communication and other related innovations are gaining tremendous growth in the modern technological era. Technology development has made it more important than ever to protect citizens from a variety of threats. To address this issue, video surveillance systems have been implemented, which, while integrated with the Internet of Things, have greatly improved people's quality of life. The need for IoT-based surveillance systems, also known as smart surveillance systems, has increased in recent years. It plays a significant role in the detection of any unlawful or anomalous occurrence in any specified location and reacts instantly through smart sensors. This study defines a comprehensive standard framework for IoT and offers a complete overview of the current IoT-based smart surveillance techniques. With a 97.5% classification accuracy for video surveillance, methods such as CNN have shown better performance, but there may still be various research challenges for video surveillance using IoT in smart cities for future researchers that should be addressed for bringing up new methodologies/technologies for the welfare of society.

Contributions of authors: General structure of the work, comparison and drafting of manuscript **– Himani Sharma;** research idea and led with overall supervision, revision – **Dr. Navdeep Kanwal.**

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The research was conducted without financial support.

Data Availability

The manuscript has no associated data.

Use of Artificial Intelligence

The authors confirm that they did not use artificial intelligence methods while creating the presented work.

All the authors have read and agreed to the published version of this manuscript.

References

1. Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Hai Tao, M., & Zolkipli, M. F. Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. *Sustain. Cities Soc.*, 2020, vol. 61, article no. 102324. DOI: 10.1016/j.scs.2020.102324.
2. Sharma, N., Shamkuwar, M., & Singh, I. The history, present and future with IoT. *Intelligent Systems Reference Library Internet of Things and Big Data Analytics for Smart Generation*, Springer, 2018, vol. 154, pp. 27-51. Available at: https://ouci.dntb.gov.ua/works/73pqrnX4/ (accessed 15 June 2023).
3. Li, S., Da Xu, L., & Zhao, S. The internet of things: a survey. *Inf. Syst. Front.*, 2015, vol. 17, no. 2, pp. 243-259. Available at: https://ideas.repec.org/a/spr/infosf/v17y2015i2d10.1007_s10796-014-9492-7.html (accessed 15 June 2023).
4. Hong, N., & Xuefeng, Z. A security framework for Internet of Things based on SM2 cipher algorithm. *International Conference on Computational and Information Sciences, ICCIS 2013*, 2013, pp. 13-16. DOI: 10.1109/ICCIS.2013.12.
5. Khan, Z., Anjum, A., Soomro, K., & Tahir, M. A. Towards cloud based big data analytics for smart future cities. *Journal of Cloud Computing*, 2015, vol. 4, no. 1, article no. 2, pp. 381-386. DOI: 10.1186/s13677-015-0026-8.
6. Ahamad, R., & Mishra, K. N. Hybrid approach for suspicious object surveillance using video clips and UAV images in cloud-IoT-based computing environment. *Cluster Computing*, 2023, pp. 1-25. Available at: https://ouci.dntb.gov.ua/en/works/96wD2wo7/ (accessed 15 June 2023).
7. Barannik, V., Krasnorutsky, A., Kolesnik, V., Barannik, V., Pchelnikov, S., & Zeleny, P. Method of Compression and Ensuring the Fidelity of Video Images in Infocommunication Networks. *Radioelectron. Comput. Syst.*, 2022, no. 4, pp. 129-142. DOI: 10.32620/reks.2022.4.10.
8. Xu, L. D., He, W., & Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Informatics*, 2014, vol. 10, no. 4, pp. 2233-2243. DOI: 10.1109/TII.2014.2300753.
9. Jia, X., Feng, Q., Fan, T., & Lei, Q. RFID technology and its applications in Internet of Things (IoT). *2nd International Conference on Consumer*

Electronics, Communications and Networks (CECNet), Yichang, China, 2012, pp. 1282-1285. DOI: 10.1109/CECNet.2012.6201508.

10. Li, S., Xu, L. D., & Wang, X. Compressed sensing signal and data acquisition in wireless sensor networks and Internet of Things. *IEEE Trans. Ind. Informatics*, 2013, vol. 9, no. 4, pp. 2177-2186. DOI: 10.1109/TII.2012.2189222.

11. He, W., & Xu, L. D. Integration of distributed enterprise applications: A survey. *IEEE Trans. Ind. Informatics*, 2014, vol. 10, no. 1, pp. 35-42. DOI: 10.1109/TII.2012.2189221.

12. Ashton, K. That 'Internet of Things' Thing. *RFID J.*, 2009, vol. 22, no. 7, pp. 97-114. Available at: http://www.rfidjournal.com/articles/view?4986 (accessed 15 June 2023).

13. Shen, G., & Liu, B. The visions, technologies, applications and security issues of Internet of Things. *International Conference on E-Business and E-Government (ICEE)*, Shanghai, China, 2011, pp. 1867–1870. DOI: 10.1109/ICEBEG.2011.5881892.

14. Gibson, D. V., Kozmetsky, G., & Smilor, R. W. *The Technopolis Phenomenon: Smart Cities, Fast Systems, Global Networks*. Rowman & Littlefield Publishers, 1992. 234 p. ISNB: 9780847677580.

15. Vinod Kumar, T. M. Smart environment for smart cities. *Advances in 21st Century Human Settlements*. Springer, 2020, pp. 1-53. ISBN: 978-9811368219.

16. Kulkarni, P. *Evolution of Internet of Things (IoT) - A Brief History*. Available at: https://bytebeam.io/blog/a-brief-history-of-internet-of-things/ (accessed 15 June 2023).

17. Yaqoob, I., Ahmed, E., Hachem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges. *IEEE Wirel. Commun.*, 2017, vol. 24, iss. 3, pp. 10-16. DOI: 10.1109/MWC.2017.1600421.

18. Wu, M., Lu, T.-J., Ling, F.-Y., Sun, J., & Du, H.-Y. Research on the architecture of Internet of Things. *3rd international conference on advanced computer theory and engineering (ICACTE)*, Chengdu, 2010, vol. 5, pp. V5-484 - V5-487. DOI: 10.1109/ICACTE.2010.5579493.

19. Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J., & Williams, P. Foundations for Smarter Cities. *IBM J. Res. Dev.*, 2010, vol. 54, iss. 4, pp. 1-16. DOI: 10.1147/JRD.2010.2048257.

20. Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. IoT in smart cities: A survey of technologies, practices and challenges. *Smart Cities*, 2021, vol. 4, no. 2, pp. 429-475. DOI: 10.3390/smartcities4020024.

21. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, Fourthquarter, 2015, vol. 17, no. 4, pp. 2347-2376. DOI: 10.1109/COMST.2015.2444095.

22. Zhang, M., Sun, F., & Cheng, X. Architecture of Internet of Things and its key technology integration based-on RFID. *5th International Symposium on Computational Intelligence and Design, ISCID 2012*, Hangzhou, China, 2012, vol. 1, pp. 294-297. DOI: 10.1109/ISCID.2012.81.

23. Kassab, W., & Darabkh, K. A. A-Z survey of Internet of Things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, 2020, vol. 163, article no. 102663. DOI: 10.1016/j.jnca.2020.102663.

24. Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, 2019, vol. 21, no. 3, pp. 2794-2830. DOI: 10.1109/COMST.2019.2899617.

25. Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine*, 2017, vol. 55, no. 1, pp. 122-129. DOI: 10.1109/MCOM.2017.1600267CM.

26. Al Zamil, M. G. H., Samarah, S. M. J., Rawashdeh, M., & Hossain, M. A. An ODT-based abstraction for mining closed sequential temporal patterns in IoT-cloud smart homes. *Cluster Comput.*, 2017, vol. 20, no. 2, pp. 1815-1829. DOI: 10.1007/s10586-017-0837-0.

27. Hou, L., Zhao, S., Xiong, X., Zheng, K., Chatzimisios, P., Hossain, M. S., & Xiang, W. Internet of Things Cloud: Architecture and Implementation. *IEEE Communications Magazine*, 2016, vol. 54, no. 12, pp. 32-39. DOI: 10.1109/MCOM.2016.1600398CM.

28. Myagmar-Ochir, Y., & Kim, W. A survey of video surveillance systems in smart city. *Electronics*, 2023, vol. 12, no. 17, article no. 3567. DOI: 10.3390/electronics12173567.

29. Raju, J. V. N., & Harini, P. Smart Video Security Surveillance with Mobile Remote Control. *International Journal of Emerging Trends in Engineering Research*, 2015, vol. 3. no. 10, pp. 169-173. Available at: http://www.warse.org/IJETER/static/pdf/Issue/icacsse2015sp30.pdf (accessed 15 June 2023).

30. Anagnostopoulos, T., Kostakos, P., Zaslavsky, A., Kantzavelou, I., Tsotsolas, N., & Salmon, I. Challenges and solutions of surveillance systems in IoT-enabled smart campus: a survey. *IEEE Access*, 2021,

vol. 9, pp. 131926-131954. DOI: 10.1109/ACCESS.2021.3114447.

31. Rao, B. N., & Sudheer, R. Surveillance camera using IoT and Raspberry Pi. *Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2020, pp. 1172-1176. DOI: 10.1109/ICIRCA48905.2020.9182983.

32. Jeličić, V., Magno, M., Brunelli, D., Bilas, V., & Benini, L. An energy efficient multimodal wireless video sensor network with eZ430-RF2500 modules. *5th International Conference on Pervasive Computing and Applications (ICPCA10)*, Maribor, Slovenia, 2010, pp. 161-166. DOI: 10.1109/ICPCA.2010.5704091.

33. Saraceni, S., Claudi, A., & Dragoni, A. F. An active monitoring system for real-time face-tracking based on mobile sensors. *Proceedings Elmar - International Symposium Electronics in Marine*, 2012, pp. 53-56. Available at: https://www.researchgate.net/publication/235965503_An_Active_Monitoring_System_for_Real-Time_Face-Tracking_based_on_Mobile_Sensors (accessed 15 June 2023).

34. Mekonnen, T., Harjula, E., Koskela, T., & Ylianttila, M. SleepyCAM: Power management mechanism for wireless video-surveillance cameras. *IEEE International Conference on Communications Workshops (ICC Workshops*), Paris, France, 2017, pp. 91-96. DOI: 10.1109/ICCW.2017.7962639.

35. Mekonnen, T., Harjula, E., Heikkinen, A., Koskela, T., & Ylianttila, M. Energy Efficient Event Driven Video Streaming Surveillance Using SleepyCAM. *IEEE International Conference on Computer and Information Technology (CIT)*, Helsinki, Finland, 2017, pp. 107-113. DOI: 10.1109/CIT.2017.10.

36. Nath, R. K., Bajpai, R., & Thapliyal, H. IoT based indoor location detection system for smart home environment. *IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, USA, 2018, pp. 1-3. DOI: 10.1109/ICCE.2018.8326225.

37. Gallo, P., Pongnumkul, S., & Nguyen, U. Q. BlockSee: Blockchain for IoT Video Surveillance in Smart Cities. *IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe, (EEEIC/I & CPS Europe)*, Palermo, Italy, 2018, pp. 1-6. DOI: 10.1109/EEEIC.2018.8493895.

38. Mao, L., Sheng, F., & Zhang, T. Face Occlusion Recognition with Deep Learning in Security Framework for the IoT. *IEEE Access*, 2019, vol. 7, pp. 174531–174540. DOI: 10.1109/ACCESS.2019.2956980.

39. AL Zamil, M. G. H., Samarah, S., Rawashdeh, M., Karime, A., & Hossain, M. S. Multimedia-oriented action recognition in Smart City-based IoT using multilayer perceptron. *Multimed. Tools Appl.*, 2019, vol. 78, no. 21, pp. 30315-30329. DOI: 10.1007/s11042-018-6919-z.

40. Roque, G., & Padilla, V. S. LPWAN Based IoT Surveillance System for Outdoor Fire Detection. *IEEE Access*, 2020, vol. 8, pp. 114900-114909. DOI: 10.1109/ACCESS.2020.3003848.

41. Desnanjaya, I. G. M. N., & Arsana, I. N. A. Home security monitoring system with IoT-based Raspberry Pi. *Indones. J. Electr. Eng. Comput. Sci.*, 2021, vol. 22, no. 3, pp. 1295-1302. DOI: 10.11591/ijeecs.v22.i3.pp1295-1302.

42. Ravikumar, S., & Kavitha, D. RETRACTED ARTICLE: IoT based home monitoring system with secure data storage by Keccak–Chaotic sequence in cloud server. *J. Ambient Intell. Humaniz. Comput.*, 2021, vol. 12, no. 7, pp. 7475-7487. DOI: 10.1007/s12652-020-02424-x.

43. Suhaimi, A. F., Yaakob, N., Ali Saad, S., Sidek, K. A., Elshaikh, M. E., Dafhalla, A. K. Y., Lynn, O. B., & Almashor, M. IoT Based Smart Agriculture Monitoring, Automation and Intrusion Detection System. *Journal of Physics: Conference Series, The 1st International Conference on Engineering and Technology (ICoEngTech) 15-16 March 2021*, Perlis, Malaysia, 2021, vol. 1962, no. 1, article no. 12016. DOI: 10.1088/1742-6596/1962/1/012016.

44. Kumar, M., Raju, K. S., Kumar, D., Goyal, N., Verma, S., & Singh, A. An efficient framework using visual recognition for IoT based smart city surveillance. *Multimed. Tools Appl.*, 2021, vol. 80, no. 20, pp. 31277-31295. DOI: 10.1007/s11042-020-10471-x.

45. Altowaijri, A. H., Alfaifi, M. S., Alshawi, T. A., Ibrahim, A. B., & Alshebeili, S. A. A privacy-preserving IoT-based fire detector. *IEEE Access*, 2021, vol. 9, pp. 51393-51402. DOI: 10.1109/ACCESS.2021.3069588.

46. Safi, A., Ahmad, Z., Jehangiri, A. I., Latip, R., Zaman, S. K. U., Khan, M. A., & Ghoniem, R. M. A Fault Tolerant Surveillance System for Fire Detection and Prevention Using LoRaWAN in Smart Buildings. *Sensors*, 2022, vol. 22, no. 21, article no. 8411. DOI: 10.3390/s22218411.

47. Rajavel, R., Ravichandran, S. K., Harimoorthy, K., Nagappan, P., & Gobichettipalayam, K. R. IoT-based smart healthcare video surveillance system using edge computing. *J. Ambient Intell. Humaniz. Comput.*, 2022, vol. 13, no. 6, pp. 3195-3207. DOI: 10.1007/s12652-021-03157-1.

48. Islam, M., Dukyil, A. S., Alyahya, S., & Habib, S. An IoT Enable Anomaly Detection System for Smart City Surveillance. *Sensors*, 2023, vol. 23, no. 4, article no. 2358. DOI: 10.3390/s23042358.

49. Meddeb, H., Abdellaoui, Z., & Houaidi, F. Development of surveillance robot based on face recognition using Raspberry-PI and IoT. *Microprocess.*

Microsyst., 2023, vol. 96, article no. 104728. DOI: 10.1016/j.micpro.2022.104728.

50. Greene, S., Thapliyal, H., & Carpenter, D. IoT-Based fall detection for smart home environments. *IEEE International Symposium on Nanoelectronic and Information Systems (INIS),* Gwalior, India, 2016, pp. 23-28. DOI: 10.1109/iNIS.2016.017.

Received 17.07.2023, Accepted 20.02.2024

РОЗУМНЕ ВІДЕОСПОСТЕРЕЖЕННЯ ЗА ДОПОМОГОЮ ІНТЕРНЕТУ РЕЧЕЙ: ОГЛЯД

Хімані Шарма, Навдіп Канвал

У сучасному суспільстві впровадження систем відеоспостереження є тенденцією, яка може революціонізувати багато технологій, особливо в розумних містах майбутнього. Навіть добре навченим співробітникам може бути важко обробляти дані, що відстежуються, і негайно реагувати на них, але інтелектуальні системи відеоспостереження на основі інтернету речей (IoT) можуть успішно з’єднати екосистеми, забезпечуючи покращений моніторинг служб розумного міста. Ця стаття містить огляд кількох методів спостереження на основі IoT, які використовуються в різних програмах розумного міста. Враховуючи історичний контекст, аналізуються дослідження, досвід використання IoT в розумних містах. Представлено архітектуру розумного міста на основі IoT, надано аналіз поточних інтелектуальних систем спостереження на основі IoT, а також визначено низку проблем, важливих для їх дослідження. Окреслено перспективні напрями розвитку систем відеоспостереження.

Ключові слова: розумні міста; система відеоспостереження; виявлення підробки відео; архітектура IoT.

Хімані Шарма – дослідник, Департамент комп’ютерних наук та інженерії, Пенджабський університет Патіала, Пенджаб, Індія.

Навдіп Канвал – проф., доц. каф. комп’ютерних наук та інженерії, Пенджабський університет Патіала, Пенджаб, Індія.

Himani Sharma – Research Scholar, the Department of Computer Science & Engineering, Punjabi University Patiala, Punjab, India,
e-mail: himanisharma781@gmail.com, ORCID: 0000-0003-3796-8501.

Navdeep Kanwal – Dr., Assistant Professor, the Department of Computer Science & Engineering, Punjabi University Patiala, Punjab, India,
e-mail: navdeepkanwal@gmail.com, ORCID: 0000-0003-3015-2390.