Irish Interdisciplinary Journal of Science & Research (IIJSR)
Volume 7, Issue 4, Pages 38-46, October-December 2023

Synergizing IoT, IoE, GSM Technology, and Deep Learning Models for Advanced Security Applications: A Comprehensive Overview

Kabilan M.[1*], Manikandan V.[2] & Suresh Kumar K.[3]

[1,2]UG Scholar, [3]Associate Professor, [1-3]Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram, India. Corresponding Author (Kabilan M.) Email: kabilan2004.7@gmail.com[*]

DOI: https://doi.org/10.46759/IIJSR.2023.7406

Article Received: 26 August 2023 *Article Accepted: 16 November 2023* *Article Published: 27 November 2023*

ABSTRACT

Technology is rapidly advancing, with a myriad of applications benefiting society across various domains. A crucial aspect of this technological evolution lies in security-related applications, where cutting-edge advancements have played a pivotal role. The backbone of many modern security systems is formed by the Internet of Things (IoT), leveraging its capabilities for seamless automation. IoT establishes a robust data network, interconnecting diverse objects like sensors, radio frequency components, smart appliances, and computers through the Internet. The Internet of Everything (IoE) represents a significant evolution of IoT, encompassing the integration of data, people, processes, and physical devices. Within this intricate system, sensors are employed to detect any unauthorized movements in scenarios where authorized personnel are absent. Complementing this, monitoring cameras serve as an alerting system. To enhance the system's capabilities, a GSM module is incorporated to facilitate the transfer of information. Deep learning models, specifically pre-trained in the proposed system, significantly contribute to the system's efficacy. Leveraging deep learning algorithms enhances the system's ability to discern and respond to complex patterns and anomalies. Notably, Region-based Convolutional Neural Networks (RCNN) are employed to capture and process images, adding a layer of sophistication to the system's overall functionality. This amalgamation of IoT, IoE, GSM technology, and deep learning models underscores the technological prowess harnessed for the advancement of security applications.

Keywords: Internet of Things; GSM Module; Recurrent Convolutional Neural Network (RCNN); Internet of Everything.

1. Introduction

In this cutting edge period the measure of crime percentage is expanding rapidly. In ongoing review around America there are about 1,190,704 violations were occurred. Because of this wrong doing $14.3 billion property misfortunes were happened. The example for the heterogeneous information can be delighted because of wrongdoing events. And because of this the security level. After the obstruction of safety date experiences there are arranged into two sorts [1]. They are: strategy related and information related. The significant defect with this sort of game plan is that it requests the every minute of every day accessibility of a house proprietor or part, or manual video observation, which is nearly unthinkable. Likewise, it is a monotonous errand to go through all the recorded video cuts after a potential burglary has become known. It is possible that the capacity worker contains a lot of relative film, which is of no utilization in recognizing intruders [2]. So catch picture shipped off police and approved individual. A framework ought to be planned which can defeat all the drawback of the existing frameworks by and by at present. The integration of cutting-edge technologies has ushered in a new era in the realm of security applications. This comprehensive overview explores the synergistic collaboration of Internet of Things (IoT), Internet of Everything (IoE), GSM (Global System for Mobile Communications) technology, and advanced deep learning models. The amalgamation of these technologies holds tremendous potential to redefine and elevate the capabilities of security systems [3]. The Internet of Things (IoT) serves as a foundational pillar, providing a robust data network that interconnects a diverse array of objects, ranging from sensors to smart appliances, all seamlessly connected via the Internet. Building upon the IoT framework, the Internet of Everything (IoE) represents an evolutionary step forward, integrating not only physical devices but also data, people, and processes

[4]. In this advanced security paradigm, GSM technology plays a vital role by empowering the system with efficient communication capabilities. The integration of GSM modules enables the secure and rapid transfer of information, enhancing the responsiveness and reach of the security infrastructure. A key innovation in this comprehensive security approach is the incorporation of pre-trained deep learning models. Deep learning, a subset of artificial intelligence, brings a heightened level of intelligence and adaptability to the security system. The models, having undergone pre-training, are adept at discerning intricate patterns and anomalies, significantly enhancing the system's ability to respond effectively to varying security challenges [5].

A focal point of the deep learning integration is the utilization of Region-based Convolutional Neural Networks (RCNN), which prove instrumental in capturing and processing images. This not only adds a layer of sophistication to the system but also enables a nuanced understanding of the surrounding environment. This comprehensive overview delves into the intricacies of how these technologies collaboratively contribute to the advancement of security applications. From IoT's foundational connectivity to IoE's holistic integration, GSM's communication prowess, and the intelligence brought forth by deep learning models, this synergistic approach promises a paradigm shift in the landscape of security systems [6]. As we navigate through the nuances of this integration, a deeper understanding emerges of the transformative potential these technologies hold for the future of advanced security applications. This task conquers the weaknesses of above notice strategy to discover of wrongdoing occurring. Late demonstrations of burglary/psychological warfare have featured the dire requirement for effective video reconnaissance and on-the-spot notice of progressing burglaries to house proprietors and other family individuals [7]. Various reconnaissance arrangements are right now accessible available, like CCTV cameras also, advanced video recorders (DVRs) that can record the unapproved exercises of an intruder, yet can’t recognize human and non- human items. With the development of troubles and difficulties, Robbery expansions in gem dealers shop, bank during shop shutting time. They have reconnaissance framework yet not successful catch the looters face because of they wear view.

2. Related Works

In recent times, the escalating rate of burglary crimes in commercial establishments such as shops and shopping malls has propelled the widespread adoption of Closed-Circuit Television (CCTV) systems. These systems have become indispensable tools in crime prevention due to their ability to deter criminals, monitor premises, and capture crucial footage of events. Whether the goal is to curtail theft and loitering in businesses or create a secure environment for residents, CCTV cameras play a pivotal role in enhancing security measures [8]. Numerous studies have explored the effectiveness of CCTV systems in deterring criminal activities. In their literature review conducted a comprehensive analysis of various case studies and reported a significant reduction in burglary rates in areas equipped with CCTV surveillance. The presence of visible cameras acted as a deterrent, dissuading potential criminals from engaging in unlawful activities [9]. This finding underscores the preventive potential of CCTV systems in safeguarding commercial spaces. Additionally, the authors investigated the impact of CCTV technology on the apprehension of criminals. Their research revealed that the use of CCTV cameras facilitated the identification and capture of perpetrators, aiding law enforcement agencies in solving crimes efficiently. The ability of these systems to provide tangible evidence proved crucial in the prosecution of offenders and the overall

enhancement of public safety [10]. In the proposed framework discussed in the present study, the focus lies on employing CCTV cameras for real-time surveillance in shops or banks during operational hours. A unique feature of the system involves activating a security mechanism during the closing hours of the establishment. When the security system is turned on, a microchip triggers a Passive Infrared (PIR) sensor, designed to detect any human presence in the vicinity. Upon detecting a human presence, the camera captures an image of the individual, which is then promptly sent to the police and authorized personnel via email. Furthermore, an alert message is generated using the Internet of Things (IoT) technology, providing an instantaneous notification of the intrusion [11].

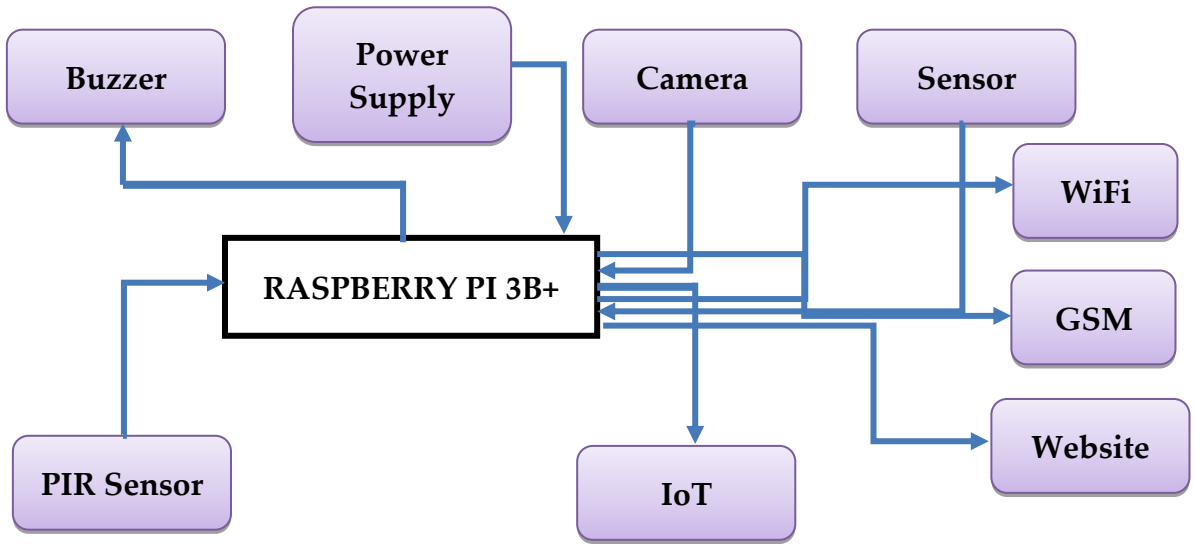
This proposed system aligns with the findings of [12], who emphasized the importance of integrating advanced technologies like IoT in security systems to enhance their efficacy. The seamless communication between the CCTV system, PIR sensor, and IoT technology enables a swift and coordinated response to potential security threats. Moreover, [13] conducted a meta-analysis of various security measures, including the use of CCTV systems, and highlighted the positive correlation between their implementation and a reduction in criminal incidents. The integration of smart technologies, as seen in the proposed framework, contributes to the adaptability and responsiveness of security systems, making them more effective in preventing and addressing criminal activities. Presently a-days the vast majority of the burglary wrongdoings happens in shops, shopping centers, and so on Also in such territories CCTV is utilized [14]. CCTV cameras are a staple in crime prevention because they help ward off criminals, monitor building premises, and record valuable footage of events. Whether you're looking to reduce theft and loitering in your business or provide a safe haven for your residents. In conclusion, the literature supports the pivotal role of CCTV systems in crime prevention and the apprehension of offenders [15]. The proposed framework, with its real-time surveillance capabilities, activation of security measures during non-operational hours, and integration of IoT technology, emerges as a comprehensive solution to address the rising concerns of burglary in commercial establishments. By leveraging the insights from existing studies, this framework not only aligns with current best practices in security but also introduces innovative features to enhance its overall effectiveness in safeguarding businesses and ensuring public safety [16]. In the proposed framework, we are doing typical observation in the shop or save money with the help of camera during working hours. During the conclusion season of the shop or bank the approved individual will turn on the security component through the page [17],[18]. When the security system is turned on, at that point the microchip will actuate the PIR sensor for recognizing any human presence around there. What's more, if any human presence is identified, at that point the camera will catch the picture of the individual entered [19]. At that point the picture of the individual will be shipped off the police and approved individual through email and furthermore ready message will be sent with the assistance of IOT. By executing this technique we can stop the robbery and furthermore ready to catch the hoodlum.

3. Proposed System

When the mechanism for the Internet of Things on the webpage is activated, the microprocessor will activate the PIR sensor as well as the camera. The PIR sensor will detect the radiation that is emitted by the person who is present in the area and will transmit this information to the computer. Additionally, the microprocessor will be able to obtain the image of the individual that was captured by the camera at the same time. Following that, the

individual who initiated the process of the Internet of Things will be sent an email containing the picture from the processor. After that, the central processing unit (CPU) causes the buzzer to sound an alarm. After that, the pump motor will release air rather than gas for the pump. In order to activate the fan and remove any airborne particles, it is necessary to disable the Internet of Things mechanism that is located on the webpage. After the processes have been carried out, the webpage will show the current status of each particular process.

3.1. Block Diagram



3.2. Buzzer

There are three different types of audio signaling devices: mechanical, piezoelectric, and electromechanical. Examples of these devices include buzzers and beepers. Changing the signal from an audio to a sound format is the primary objective of this particular process. In most cases, it is utilized in timers, alarm devices, printers, alarms, computers, and other applications that are analogous to these. It operates on direct current (DC) voltage. It is able to produce a variety of sounds, including alarm, music, bell, and siren, depending on the different designs that are available. The active buzzer is capable of producing a continuous sound when it is connected, and it operates at a voltage of around 5V. The fact that it is designed to be used in conjunction with a sensor expansion module and that it can be easily integrated into a circuit design makes it possible to have a "plug and play" experience that is both simple and convenient.

3.3. Raspberry PI 3B+

The Model B+, which is the most recent version of the Raspberry Pi 3, is the newest member of the family. This device is sure to impress thanks to its 1.4GHz 64-bit quad-core central processing unit (CPU), dual-band wireless LAN (WLAN) support for both 2.4GHz and 5GHz frequencies, Bluetooth 4.2/BLE, enhanced Ethernet connectivity, and the option to utilize Power over Ethernet (PoE) with a separate PoE HAT. As a result of the modular compliance certification offered by the dual-band wireless LAN, the amount of wireless LAN compliance testing that is required to incorporate the board into finished goods is significantly reduced. Cost-effectiveness is improved, and the time it takes to bring a product to market is reduced. There is no difference between the

Raspberry Pi 3 Model B+ and the Raspberry Pi 2 Model B or the Raspberry Pi 3 Model B in terms of the physical dimensions of the Raspberry Pi. All models come equipped with a Broadcom system on a chip (SoC) that features an integrated central processing unit (CPU) that is compatible with ARM and an on-chip graphics processing unit (GPU).

3.4. Flow Chart

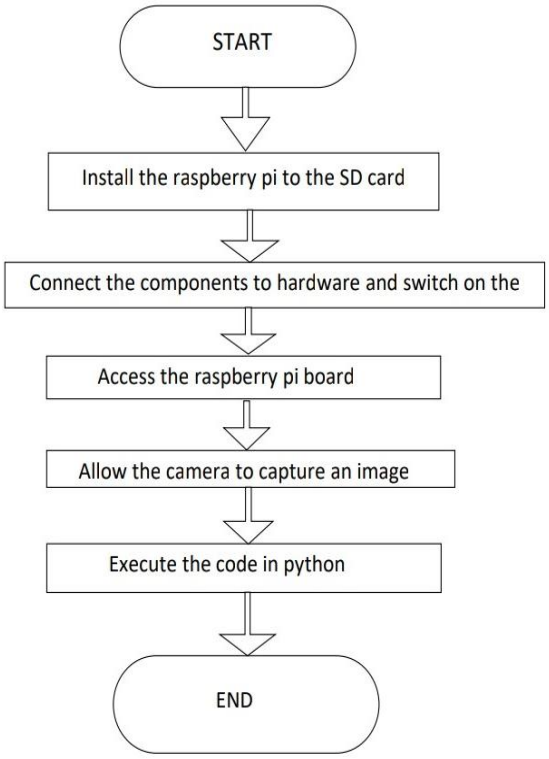


Figure 1. Flow chart

3.5. Internet of Things

The Internet of Things, also known as IoT, has emerged as one of the most significant technological advancements throughout the current century in a very short amount of time. Through the use of embedded devices, it is now possible to achieve seamless communication between people, processes, and things. This is made possible by the ability to connect commonplace items such as baby monitors, refrigerators, automobiles, and thermostats to the internet by making use of computer hardware and software that is available at reasonable prices. These devices are capable of being used for everything from commonplace items to high-tech machinery. More than seven billion Internet of Things devices are currently connected to one another, and experts forecast that this number will increase to ten billion by the year 2020 and twenty-two billion by the year 2025.

4. Results and Discussions

Machine Queuing Telemetry Transport Protocol, also known as MQTT, is the connection protocol that the Raspberry Pi and the ESP8266 use in order to communicate with one another respectively. Keeping the Internet of Things in mind, this protocol was developed. This lightweight messaging transport technique makes use of the Publish/Subscribe pattern and its associated pattern. This has a significant positive impact on connections that use

Internet Protocol (IP). By utilizing the MQTT node of Node-RED, the process of publishing and subscribing to discussion topics is simplified. "servoH," "servoV," and "Image capturing" are the keywords that are broadcast by the ESP12E. The node in Node-RED is the location where subscriptions are implemented when a Raspberry Pi is being used. As a consequence of this, the user nodes will receive the messages to which they have purchased subscriptions.

Table 1. Output Alarm Level for Various Motion and Sounds

S. No.	Motion Level	Sound Level	Theft alarm level
1	60	50	50.95238095
2	40	30	48.91472868
3	80	60	58.7804878
4	90	80	64.83870968
5	80	70	58.7804878
6	50	20	49.9999999
7	40	10	49.04761905
8	80	40	58.7804878

The Motion Level column appears to indicate the level of motion, possibly in some unit (e.g., percentage, arbitrary scale). The Sound Level column seems to represent the level of sound, possibly in some unit as well. The Theft Alarm Level column appears to be a calculated value, perhaps representing the theft alarm level, and it seems to be computed based on the values in the Motion Level and Sound Level columns.

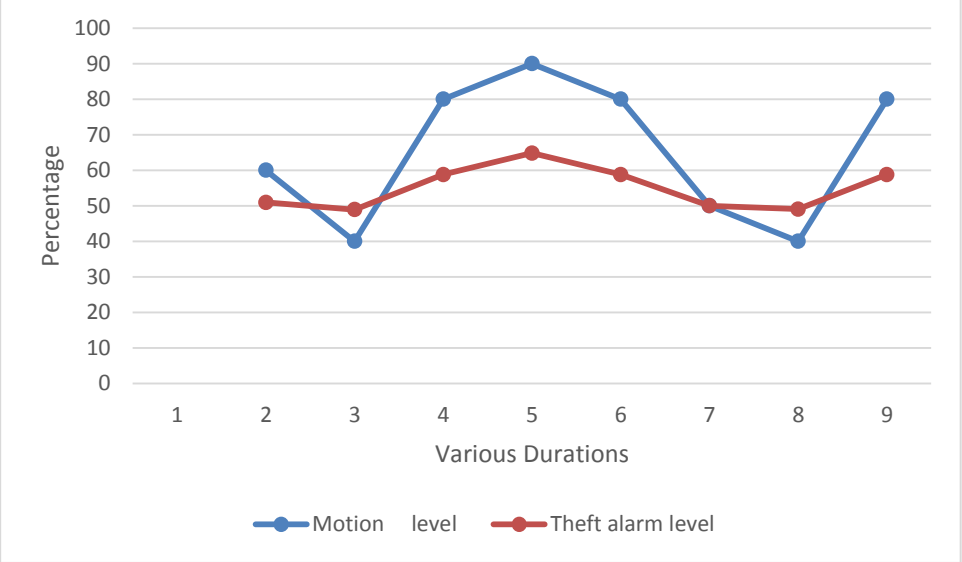


Figure 2. Theft Alarm Level for different Motions

The numbers in the "Theft Alarm Level" column seem to be calculated based on some formula or algorithm involving the values in the "Motion Level" and "Sound Level" columns. The specific formula used for this calculation is not provided, but it appears to be some kind of mathematical operation. The "Theft Alarm Level" values generally increase as the "Motion Level" and "Sound Level" increase, but the exact relationship is not clear without additional information about the calculation method. The graphical representation of the output alarm level is illustrated in Figure 2 for motion level and figure 3 for sound level.

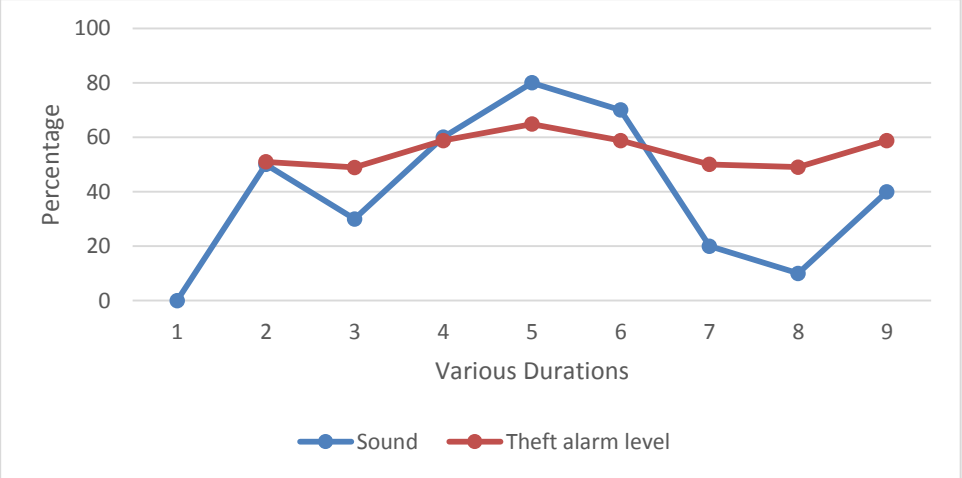


Figure 3. Theft Alarm Level for different Sounds

The numbers in the Theft Alarm Level column are expected to be the result of a calculation, possibly a mathematical operation or formula, involving the corresponding values in the Motion Level and Sound Level columns. The nature of this calculation, however, remains unspecified, leaving a gap in understanding the exact relationship between the input variables and the resulting theft alarm level. It is apparent that higher values in the Motion Level and Sound Level columns generally lead to increased values in the Theft Alarm Level column, suggesting a positive correlation. The information provides an overview of the data columns and their potential meanings, there is a critical need for a more detailed explanation of the calculation method used to derive the theft alarm level. Additional information about the graphical representations in Figure 2 and Figure 3 would also enhance the clarity of how motion and sound levels are visually represented. A comprehensive understanding of these aspects is essential for the meaningful interpretation and application of the presented data in the context of theft alarm systems.

5. Conclusions

In conclusion, the rapid evolution of technology has ushered in a new era of security applications that significantly benefit society across diverse domains. At the forefront of these advancements is the Internet of Things (IoT), providing a robust foundation for seamless automation in security systems. The progression from IoT to the Internet of Everything (IoE) marks a significant leap, integrating data, people, processes, and physical devices into a cohesive network. Within this intricate system, sensors play a pivotal role in detecting unauthorized movements, especially in situations where authorized personnel are absent. The synergy of monitoring cameras and a GSM module further amplifies the system's capabilities, serving as a comprehensive alerting system with the ability to

transfer information efficiently. A standout feature of the proposed system is the integration of deep learning models, specifically pre-trained for optimal performance. This strategic incorporation enhances the system's efficacy by enabling it to discern and respond to complex patterns and anomalies. The utilization of Region-based Convolutional Neural Networks (RCNN) adds a layer of sophistication to the system's image processing capabilities, elevating its overall functionality. The amalgamation of IoT, IoE, GSM technology, and deep learning models represents a testament to the technological prowess harnessed for the advancement of security applications. This convergence not only strengthens the capabilities of security systems but also underscores the adaptability and responsiveness required to address the evolving challenges in ensuring safety and protection. As technology continues to progress, the symbiotic relationship between these cutting-edge components is poised to redefine the landscape of security, offering innovative solutions to safeguard society in an increasingly interconnected world.

Declarations

Source of Funding

This study has not received any funds from any organization.

Conflict of Interest

The authors declare that they have no conflict of interest.

Consent for Publication

The authors declare that they consented to the publication of this study.

Authors' Contribution

All the authors took part in literature review, research, and manuscript writing equally.

References

[1] Li, D., Liang, B., & Zhang, W. (2014). Real-time moving vehicle detection, tracking, and counting system implemented with OpenCV. IEEE Int. conference on information science and technology, Pages 631–634, IEEE.

[2] Sorwar, T., Azad, S.B., Hussain, S.R., & Mahmood, A.I. (2017). Real-time Vehicle monitoring for traffic surveillance and adaptive change detection using Raspberry Pi camera module. In 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Pages 481–484, IEEE.

[3] Chauhan, N.S., Rahman, F., Sarker, R., & Pious, M.M.H. (2018). Vehicle detection, tracking and counting using linear quadratic estimation technique. In 2018 2nd International Conference on Inventive Systems and Control (ICISC), Pages 603–607, IEEE.

[4] Yang, H., & Qu, S. (2018). Real-time vehicle detection and counting in complex traffic scenes using background subtraction model with low-rank decomposition. IET Intelligent Transport Systems, 12(1): 75–85.

[5] Soleh, M., Jati, G., Sasongko, A.T., Jatmiko, W., & Hilman, M.H. (2017). A real time vehicle counting based on adaptive tracking approach for highway videos. In 2017 International Workshop on Big Data and Information Security (IWBIS), Pages 93–98, IEEE.

[6] Preradovic, S., & Karmakar, N.C. (2010). Chipless RFID: Bar code of the future. IEEE Mic Mag., 11(7): 87–97.

[7] Zilliox, M.J., & Irizarry, R.A. (2007). A gene expression bar code for microarray data. Nature Methods, 4(11): 911–913.

[8] Paoletti, R.D., Suess, T.M., Lesko, M.G., Feroli, A.A., Kennel, J.A., Mahler, J.M., & Sauders, T. (2007). Using bar-code technology and medication observation methodology for safer medication administration. American Journal of Health-System Pharmacy, 64(5): 536–543.

[9] Falas, T., & Kashani, H. (2007). Two-dimensional bar-code decoding with camera-equipped mobile phones. In Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07), Pages 597–600, IEEE.

[10] Sundaresan, S., Suresh, K., Kishore, V., & Jayakumar, A. (2021). Insight into Various Algorithms for Medical Image Analyzes Using Convolutional Neural Networks (Deep Learning). In Handbook of Deep Learning in Biomedical Engineering and Health Informatics, Pages 137–164, Apple Academic Press.

[11] E. Joseph & T. Pavlidis (1994). Bar code waveform recognition using peak locations. IEEE Trans. PAMI, 16(6): 630–640.

[12] R. Dyachok, O. Hrytsyshyn & S. Salamaha (2017). System of Detection and Scanning Bar Codes in Panoramic Images of Raspberry Pi. 7th International Youth Science Forum LITTERIS ET ARTIBUS 2017: Computer Science & Engineering (CSE-2017), Pages 430–431.

[13] K.Q. Wang (2005). Barcode reading from images captured by camera phones. IEEE Mobility Conference.

[14] S. Sowe, E. Simmon, K. Zettsu, F. de Vaulx & I. Bojanova (2016). Cyber-Physical- Human Systems: Putting People in the Loop. IT Professional, 18(1): 10–13.

[15] L. Lamport, R. Shostak & M. Pease (2016). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3): 382–401.

[16] M. Castro & B. Liskov (2002). Practical Byzantine fault-tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), Volume 20, Number 4.

[17] Suresh Kumar, K., Radha Mani, A.S., Sundaresan, S., & Ananth Kumar, T. (2021). Modeling of VANET for future generation transportation system through Edge/Fog/Cloud computing powered by 6G. Cloud and IoT-based Vehicular Ad hoc Networks, Pages 105–124.

[18] Prabakaran, D., Nizar, S.M., & Kumar, K.S. (2021). Software-defined network (SDN) architecture and security considerations for 5G communications. In Design methodologies and tools for 5G network development and application, Pages 28–43, IGI global.

[19] Benezeth, Y., Laurent, H., Emile, B., & Rosenberger, C. (2011). Towards a sensor for detecting human presence and characterizing activity. Energy and Buildings, 43(2-3): 305–314.