ISSN 2278-3091

Volume 9, No.4, July – August 2020

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse106942020.pdf

https://doi.org/10.30534/ijatcse/2020/106942020

Design of Collaborative Framework of Network Technologies to Enhance Surveillance Security and Intrusion Detection

S.Sivachandiran[1], Dr.K.Jagan Mohan[2]

[1] Department of Computer Science and Engineering, Annamalai University, India, sivachandiran.s@gmail.com

[2]Department of Information Technology, Annamalai University, India, aucsejagan@gmail.com

ABSTRACT

Surveillance Security in recent times has been challenged with the existence of a single network technology that meets certain demands and fails to counteract the overall needs of the security systems. This problem enables intruders to easily by-pass the surveillance system and create problems in huge crowded arenas. The Major objective of this study is to design a theoretical Framework that is formed as a collaboration of various Network Technologies like Crowdsourcing, Edge Technology, Cloud enabled services, Internet of Things (IoT) along with Machine learning techniques and deep learning algorithms for attaining two major objectives via 1) Enhancement of Transmission speed in terms of Latency, Bandwidth, Transmission Speed with Delay factors; and to enhance integration of technologies in order to accept the video surveillance data in the form of clips, pre-process them using machine learning filters and finally match the objects in video with the trained set of objects using deep learning algorithms. The detailed analysis of all the techniques and their theoretical observations are discussed in the study. Such Frameworks are capable to provide optimal solutions to acquire data in time, store them and process them with optimal accuracy than the existing models.

Key words: Crowdsourcing, Edge Technologies, Video Surveillance, Machine and Deep Learning, Transmission Performance.

1. INTRODUCTION

Crowd Surveillance with Anomaly detection and image mapping is one of the challenging aspects as abnormality tend to occur especially in heavy crowd where video in real-time is hard to be diagnosed by existing algorithms and techniques as studied by [1]. The current Closed-Circuit television (CCTV) systems were installed with the ability to capture high quality video where objects could be detected clearly with accuracy. However, identification in manual mode endorses the presence of human intelligence and presence of a human data collector for a 24x7 routine. Thus, it is highly recommended to build an automated infrastructure that is capable of automatically collect the data of objects through CCTV Surveillance and enable image mapping to Machine Learning Algorithms through Cloud based Edge servers and Crowdsourced data acquisition methods.

1.1Crowdsourcing in Surveillance

Crowdsourcing is one of the imperative technologies used to acquire information or data and convert it into a task through comparison with a large group of people referred as crowd using Internet services. The data collected can be of any type ranging from normal images to intellectual information. Crowdsourcing assists in globalisation of information to large groups of people from another large groups of crowds. The crowdsourcing finds best usage in huge platforms like CCTV Surveillance over a large population and mapping the data with

another group of people. The architecture of crowdsourcing indicated in Figure 1 presents the reputation of the technique in CCTV Surveillance.

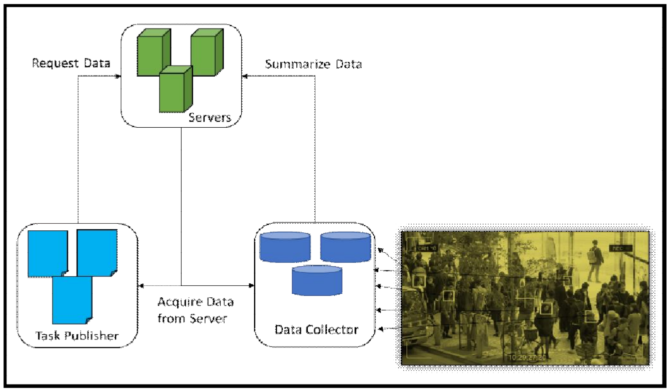

Figure 1: Architecture of Crowdsourcing applied in Crowd Surveillance

The architecture portrayed in Figure 1 indicates a three-fold model comprising of three major components viz. Data Collector, Task Publisher and Crowd Servers. The Data collector is responsible to collect the CCTV footage video from the device through cloud enabled servers and sent to the crowd servers to store and process the information. The data is acquired from server by Task Publisher to organise and perform the processing of data into required information. The server both receives and provides data to both data collector and task publisher respectively. Though these crowdsourcing techniques in crowd surveillance aids various advantages like enhancement of market, reducing management and security problems, it couldn't be automated and has to be done manually. The speed of data transmission also is not sufficient to transfer high quality video data in time.

1.2 Objective of the Research

The major objective of this study is to conduct a theoretical analysis on the possibilities of integration of various network technologies like Edge computing, Crowdsourcing, Internet of Things (IoT) and Cloud based services with crowdsourcing and machine learning based image mapping techniques to enhance security of surveillance over a region involved with huge crowd of people. The motivation is to build an infrastructure that is capable of enhancing the security surveillance with high accuracy and speed.

2. RELATED WORKS

The Integration of Technologies especially network-based technologies had been practically tested in many research studies that incorporated new dimension of hybrid technologies with better performance. [2] developed a reputation evaluation model based on Random Forest and Linear discriminant model. The model comprised of five stages including real-time datasets collection, reducing the data dimension using techniques like Linear discriminant analysis, normalisation of data, applying machine learning techniques like Decision tree, Support Vector Machines etc and finally testing the model with 10 fold cross validation and generating a confusion matrix to apply performance measures like performance and effective nature. The results indicated good performance based on identification of crowdsourcing participants that is available under bigdata environment. [3] designed a computer vision-based automated surveillance that is capable of monitoring the campus and also initiates actions once any anomalies or intrusions are detected at any point of time. The algorithm used were the face recognition algorithm and also motion detection algorithm to enhance reliability of the software in recognising the users and also identifying the intruders. The system also provides alarm when any intrusion or anomalies are detected in the camera monitor. The expected outcome was reliable and helped the police in maintaining the traffic congestions and anomalies.

An Economical surveillance system was presented by [4] with the aid of available cameras in combination with image processing techniques. An analytic was conducted on video recorded during surveillance and content analysis was performed. After the real-time analysis on assessment with every user in the surveillance camera video, it achieved best performance with 95% and the usability rate of up to 90%. This result was convincing with image sensors and image processing techniques. However, searching was not used in this surveillance system. [5] observed various visually impaired people experiencing accidents in traffic and also the social anxieties behind the problem. Based on the observations, author developed a white-cane user walking recognition technique that helped in acquiring and anticipating traffic problems to prevent accidents. The experimentation was carried out based on the images captured from the traffic signals and implemented with good results.

A Recalibration technique was designed by [6] for camera to handle discontinuous and stitched top view of camera images. The top view of surveillance images was tested for observing spatial analysis. The novel method of recalibration used to understand structural similarities and also physical changes of discontinuous images and restored images close to the original quality. This method was successfully performed using image processing methods. [7] designed a model based on deep learning algorithms to read human body and human face in two modes and developed a detection algorithm to identify and predict either the body or face match of any individual captured using a camera. The system was tested with surveillance camera outcomes and evaluated through feedbacks from various evaluators. This system was found effective even among heavy crowd, however it required complex architecture for enhanced speed and storage.

A survey of crowd analysis was conducted using techniques involving object recognition, crowd analysis, action recognition by [8] and also voice detection using deep learning techniques. Deep learning methods to count members, person's identity revealing, activity and motion detections etc. The major focus of this paper is to analyse the video obtained from surveillance using deep learning techniques and algorithms. The paper identified few issues in handling data and reducing the obstacles in the video images. However, it was not performed on real-time basis and available as survey and libraries in Science direct, IEEE Xplore and ACM digital library for further research references.

A similar surveillance camera was designed by [9] for visual surveillance monitoring system to detect anomalies or monitor specific activities in video captured through cameras. The major objective was to prevent security attacks, intrusion detections with special effects like zoom, focus and recording of motions. The cyber physical attacks develop ineffective situation among cameras that are targeted by cybercrime hackers. The physical configurations might also be altered during the problem. The detection mechanism was developed with the aid of deep learning algorithm that analysed the video obtained from surveillance camera frame by frame and apply algorithms to detect anomalies that occurred in different situation. This model enhanced the security of surveillance but speed of transmission was much slower compared to normal surveillance.

Various observations on the various advantages and disadvantages of the different components used in surveillance monitoring system based on surveys by [10]. The research survey proved that surveillance has to be enhanced with efficient algorithms and image mapping techniques for accurate mapping of images. [11] created a solution for problems experienced in single overhead camera based on frontal as well as overhead based surveillance problems. This model provided solution for enhancement of efficiency as well as accuracy of surveillance prediction. The camera was diagnosed as wide-angle lens and also single smart centralised overhead camera respectively. The final result indicated that the impact of the surveillance has been solved in terms of power consumption, storage, time efficient, human resource as well as in utilisation of less area compared to other models.

A prototype was generated by [12] that developed a surveillance system with enhanced mobility and cost efficiency system. It also detected anomalies without the aid of physical sensors and sends an alarm in the form of SMS text or E-Mail with the existing resources and space. Thus, this model provided support as well as efficiency of transmission. The utilisation of 4G technologies also is an added advantage with minimum resources. However, an enhancement in image mapping and anomaly detection was recommended.

The Literature survey glimpsed a possibility of integration of technologies including Internet-of-Things (IoT), Edge Technologies, Crowd Sourcing, Machine and Deep Learning with Cloud based services. The Transmission performance was one of the chief problems observed in many of the reviews. Hence the Transmission performance factors related to transmission of surveillance data is presented in oncoming contents.

3. SURVEILLANCE SECURTY TRANSMISSION PROBLEMS

Among the various Transmission Performance factors identified in various studies, three of the factors paves an important role in enhancing the efficiency of transmission of even huge data that comprised of video, audio or other complex data. They are explained below:

3.1 Latency

Latency is the performance factor [13] to indicate the total time taken for a data packet to move from source to destination in a networking environment. It is actually the time interval or duration between two nodes. It's also referred to as the time delay between two transmission nodes. Latency is affected by interface errors, fragments in packets, network interface port saturation, routing problems etc. Latency is generally measured in terms of milliseconds to indicate the quality of transfer between the nodes. The optimal level that can be achieved with latency is between 20 Ms and 40 Ms. The Packet Queuing is found to be one of the biggest problems faced for latency. Latency in other terms can also be indicated as throughput that measures latency per unit of time. Latency is one of the important factors to be enhanced during surveillance data comprised of huge data in the form of video frames.

3.2 Bandwidth

Bandwidth is identified as the range between the highest and lowest frequency experienced during transmission of data as suggested by [14]. The Bandwidth measured in rad per second can be calculated as indicated in Eq. (1)

$$Bandwidth\ (B) = \text{Max. Frequency} - \text{Min. Frequency}\ \textbf{Eq. (1)}$$

Bandwidth is one of the important quality factors required to monitor and evaluate the transmission power of huge data like video streaming data. To manipulate the best outcome, the effective Bandwidth needs to be calculated based on highest transmission rate that is reliable. The bandwidth is also determined by the signal availability of the network and also the device support to control routing and manage congestion during hard times of transmission. The bandwidth can also be detected wit measurements using physical components and devices using 95th Percentile method for continuous monitoring of data transmission with normal bandwidth over a period of time. It helps to boost the transmission speed for packets like video, audio that required good quality before and after transmission.

a. Transmission Speed

The Transmission speed is observed as the count of number of data or information transferred over unit period of time. It can be measured in terms of bits, characters or groups of records per second or per minute time period. The transmission speed required the values from three components viz transfer speed, time required and the amount of data transferred as given by [15]. The speed of transmission can be identified by dividing the amount of data transferred with the time period as indicated in Eq. (2).

$$Transmission\ Speed\ (TS) = \frac{Quantity\ of\ Data}{Time\ Period}\textbf{Eq. (2)}$$

The transmission speed varies from quantity of data from ordinary text to high quality video streams from satellites. The transmission delay [16] also is an important factor contrary to transmission speed to enhance video data transmission. It can be measured with the size of the data packets to be transferred and the bandwidth of the network used as indicated in Eq. (3)

$$Transmission\ Delay\ (TD) = \frac{Size\ of\ Video\ Data}{Bandwidth}\textbf{Eq. (3)}$$

However, it is highly suitable for surveillance videos where data quality can be enhanced with the use of cloud enabled services.

4. METHODOLOGY TO ENHANCE CROWD SURVEILLANCE SYSTEMS

The Methodology of the proposed Crowd Surveillance systems aims at enhancing the performance of transmission based on three factors latency, bandwidth and the transmission speed with reduced transmission delay. Hence the proposed model requires integration of network technologies to enhance efficiency of transmission.

To build a Framework model, four technologies are analysed as indicated below:

1. Edge based Technologies in Video Surveillance
2. Cloud enabled Services to transfer and Store data
3. Machine Learning Techniques for Video image processing
4. Intrusion detection using deep learning and IoT

These technologies can be integrated to form a powerful framework that is capable of enhancing the transmission performance in all aspects. The need for all these technologies is analysed in depth under distinct heads.

4.1 Edge based Technologies in Video Surveillance

Video Streams especially of high-resolution type requires high speed centralised server as well as the reliable network for efficient transfer. There is a bigger hurdle when the number of surveillance cameras increases as it might be hard for central server to handle all the clients at a time. Hence the performance of transmission specifically bandwidth gets reduced as indicated in [17]. Data compression can lead to loss of quality of data as lossless compression with less data size is still a challenging path especially in areas of crime and investigation, forensic assessments where minute information is important for accurate results.

Hence, instead of Centralised server, an Edge-based server [18] would enhance the speed and quality of transmission as well as manage the security of data. The edge server moves video data into a server with digital capture of video or images much easier compared to traditional system of decentralised system which required huge infrastructure of cost and maintenance. The Edge servers utilises high speed computers and data cards to store and process the video even in highly congested network environment.

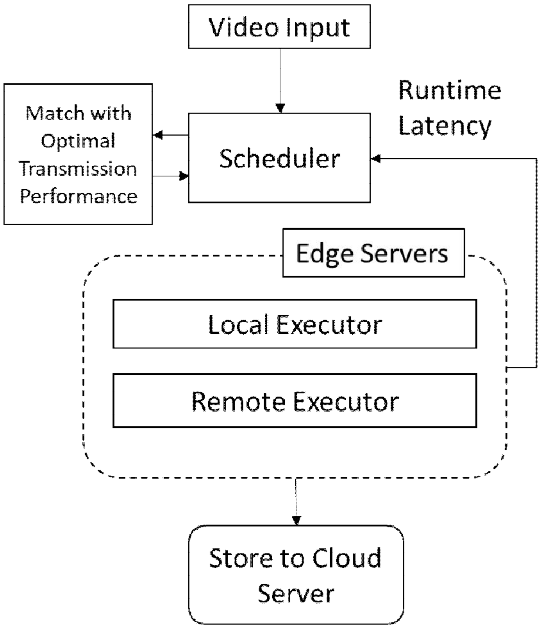

Figure 2: Edge Enabled Video Storage Server

The schematic diagram showed in Figure 2 indicates the Transmission performance analysis through scheduler to match the optimal user requirements for every data packet transferred to either local or remote Edge Server. The accuracy of transmission quality and speed can be enhanced with Edge servers as they are considered as intelligent servers that uses digital technologies for more advanced images with more clarity in video and pictures.

The major problem of achieving the quality and performance of transmission can be achieved with the help of edge-based Surveillance compared to centralised surveillance that is prevalent over the years. However, for remote storage of high-quality data over edge network, the cloud enabled services plays a significant role specifically in case of multiple surveillance results at the same time.

4.2 Cloud enabled Services to transfer and Store data

As many open source services and servers are fast imminent in recent technologies, Cloud based video surveillance as given by [19] is considered more efficient and potential compared to other servers due to high utilisation of bandwidth in cloud-based infrastructure. It is also cost effective and secured for all kinds of enterprise solutions either small or large to store and process huge amount of data.

Based on the feasibility of software, hardware support and assessing of video data on time, cloud enabled server provides best support for quality in compression and storing the data at a faster rate compared to other servers. The cloud-based servers for storage are also associated with direct transfer of data from time to time as and when required for instant support. The cloud can also manage the data bandwidth, cost of installation, security through proper authentication and promoting accessibility of data in time through pre-existing software application which are available with the package.

4.3 Machine Learning Techniques for Video image processing

Machine Learning enables automation of machines to act like human brain in incorporating the knowledge through attainment of self-based learning.

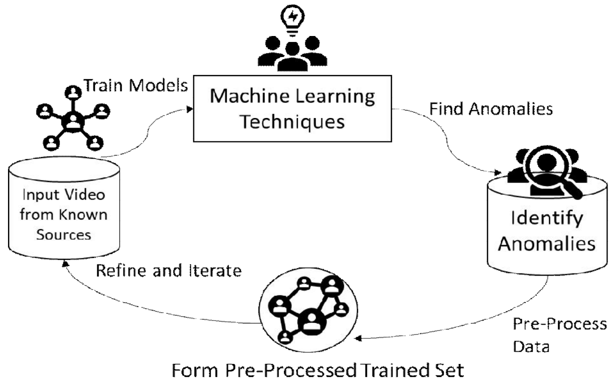
Train Models
Machine Learning Techniques
Find Anomalies
Input Video from Known Sources
Identify Anomalies
Refine and Iterate
Pre-Process Data
Form Pre-Processed Trained Set

Figure 3: Pre-Processing process for Video data using Machine Learning

As indicated in Figure 3, the input video accepted from surveillance sources stored in cloud is obtained and modelled with respective features. The image in video can be manipulated as frames and capture the image that has the object removing the unwanted frames in the form of anomalies without objects, using dense neural network techniques. Later the pre-processing techniques to avoid noisy data, blurred data can be found and removed. This helps in pre-processing the input video data that is ready for mapping using deep learning techniques.

Hence Artificially enabled systems could enhance the video data through frame by frame filters and thereby prevent unnecessary components to be used as testing frames for video mapping. Machine Learning as shown by [20] could utilise image processing through neural network algorithms like

VGG16, VGG19, ResNet50, Xception, InceptionV3 and train them in pre-existing dataset from already created models.

4.4 Intrusion detection using Deep Learning and IoT

Video surveillance applications with deep learning assists in mapping the image objections and identify the intruders with right identification from a trained dataset. The deep learning assists in mapping the objects under two aspects:

4.4.1Face Recognition

Deep learning is capable of identifying the face of a person in a close-up video recording based on existing deep learning algorithms where the accuracy of matching reached maximum level as shown in [21] provided the video is pre-processed with good normalisation procedures and noise removal process.

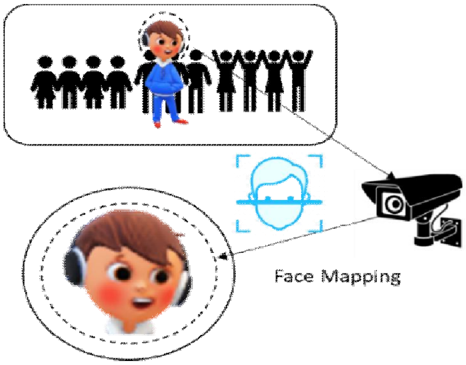

Figure 4 : Face Recognition from CCTV Camera

As shown in Figure 4, the pattern is applied in the face among the crowd captured through video of CCTV surveillance and the right face is identified.

4.4.2 Object Recognition

Object recognition among a crowd is also one of the major areas where deep learning has shown huge enhancement over the years. The pre-existing algorithms and software detect the objects based on trained set, classify them using algorithms and place them in respective database for future references. In a particular sequence, it can match more objects in a crowd and give the right matched object as suggested by [22]. After mapping, the hardware peripherals from Internet of things (IoT) are capable of accepting the acknowledgement and sending the alarms to the respective administrations who require mapping of objects. The major benefit of using deep learning algorithms is that it gets trained from time to time and enhances through self-learning. The accuracy is also capable of increasing at all levels in course of time.

Thus, the possibilities of integration of all these technologies could successfully develop an infrastructure that will be capable of enhancing the performance of video surveillance to prevent intrusions and promote security.

5. FRAMEWORK MODEL TO COLLABORATE NETWORK TECHNOLOGIES

Based on the impact analysed through literature reviews and the assessment of various potentials from all the technologies, the framework model for collaboration of various Network Technologies for video surveillance mapping is proposed.

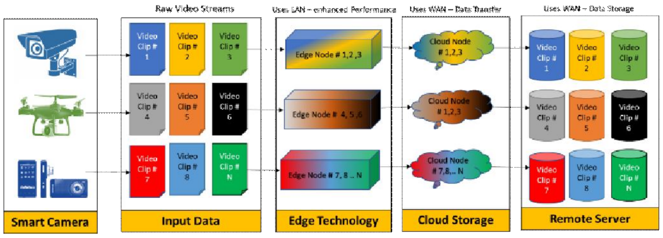

Figure 5 : Framework Model for integration of Network Technologies to enhance performance of Video surveillance transfer and storage

The framework Model as portrayed in Figure 5 comprised of three levels where the initial stage acquires the video clips as input that ranges from 1 to n clips during a particular time interval. The Clips are formed as set of components range as indicated in (4).

$$VD = \{1, 2, 3, 4, 5, 6, 7, 8\ldots N\} \qquad \textbf{Eq. (4)}$$

Where N represents the maximum limit of video data permissible at a time. The clips stores data with equal length and same size. The data input is compartmentalised and stored with three columns and ‘N’ rows as noted in Eq. (4).

$$VD1 = \{1,2,3\},$$

$$VD2 = \{4,5,6\},$$

$$VD3= \{7,8,9\},$$

$$VD4= \{N-2, N-1, N\}\textbf{Eq. (5)}$$

Where N-1 and N-2 represents previous video clips of the data stored as input. In the Second stage, the stored data are transferred to Edge enabled servers to enhance Latency with scheduler matching to optimal latency level during transmission. The Edge Server is a localised server made of Local Area Network (LAN) available in the CCTV arena as shown in [24]. A similar technique was earlier proved for possibility to find suspicious activities using integration of networks and deep learning by [25] Later the data is transferred to the cloud server as indicated in level three to boost the bandwidth and reduce the anomalies of data transmission. finally, the transferred data is stored in cloud server after segregation into various individual video clips as given in Eq.3. The Framework model is the beginning of a complete infrastructure where Machine Learning models will be applied on the data stored in cloud server and then mapped with video using deep learning techniques that might provide the match of face or object to the maximum accuracy possible.

Though the proposed framework is a theoretical formulation to enhance the transmission performance using integration of technologies, the best outcome has to be achieved under three areas using design of algorithms. The three areas are enhancement of Transmission Performance, Pre-Processing of video data with Machine Learning filters and Video Mapping using deep learning techniques.

5. CONCLUSION

The Framework Model proposed in the paper is a novel concept that has several advantages like low cost infrastructure with maximum performance with latency in case of crowd and Edge based servers, optimal bandwidth as in case of Cloud enabled services, pre-processing to remove noisy data and enhance outcomes based on machine learners and finally mapping of objects or face images using deep learning techniques to provide solution to the model with highest level of automatic security possible in video surveillance in highly populated crowd environment. The theoretical framework model is built into a prototype and has to be implemented as a technology exclusive for CCTV surveillance for intrusion detections in the near future.

REFERENCES

1. Wang, J., & Xu, Z. (2015). **Crowd anomaly detection for automated video surveillance.**
2. Huang, Y., & Chen, M. (2019). **Improve Reputation Evaluation of Crowdsourcing Participants Using Multidimensional Index and Machine Learning Techniques**. IEEE Access, 7, 118055-118067. https://doi.org/10.1109/ACCESS.2019.2933147
3. Ng, R. C., Lim, K. M., Lee, C. P., & Razak, S. F. A. (2019). **Surveillance system with motion and face detection using histograms of oriented gradients.** Indonesian Journal of Electrical Engineering and Computer Science, 14(2), 869-876.
4. Razalli, H., Alkawaz, M. H., & Suhemi, A. S. (2019, December). **Smart IOT Surveillance Multi-Camera Monitoring System.** In 2019 IEEE 7th Conference on Systems, Process and Control (ICSPC) (pp. 167-171). IEEE. DOI: 10.1109/ICSPC47137.2019.9067984
5. Sanada, K., Takizawa, H., Aoyagi, M., Ohya, A., & Kobayashi, M. (2020, March). **Recognition of White-Cane Users from Surveillance Camera Images Based on Detection of Line Segments.** In 2020 IEEE 2nd Global Conference on Life Sciences and Technologies **(LifeTech)** (pp. 268-271). IEEE. DOI: 10.1109/LifeTech48969.2020.1570616603
6. Minagawa, J., Okahara, K., Yamazaki, K., & Fukasawa, T. (2019, September). **A Camera Recalibration Method for a Top-View Surveillance System based on Relative Camera Pose and Structural Similarity.** In 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (pp. 1-8). IEEE. DOI: 10.1109/AVSS.2019.8909870
7. Alajrami, E., Tabash, H., Singer, Y., & El Astal, M. T. (2019, October). **On using AI-Based Human Identification in Improving Surveillance System Efficiency. In 2019 International Conference on Promising Electronic Technologies (ICPET)** (pp. 91-95). IEEE. DOI: 10.1109/ICPET.2019.00024
8. Sreenu, G., & Durai, M. S. (2019). **Intelligent video surveillance: a review through deep learning techniques for crowd analysis. Journal of Big Data,** 6(1), 48. **DOI:**https://doi.org/10.1186/s40537-019-0212-5
9. Pan, J. (2019). **Physical Integrity Attack Detection of Surveillance Camera with Deep Learning Based Video Frame Interpolation.** arXiv preprint arXiv:1906.06475.
10. Kalaiselvi, N., Shanmugasundaram, G., Arutselvi, P., & Kowsalya, N. (2019, March). **A Survey on Theft Surveillance and Detection Technologies**. In 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) (pp. 1-6). IEEE. DOI: 10.1109/ICSCAN.2019.8878734
11. Ahmad, M., Ahmed, I., Ullah, K., Khan, I., Khattak, A., & Adnan, A. (2019). **Energy efficient camera solution for video surveillance**. Int J Adv Comput Sci Appl, 10(3).
12. Sarrafpour, B. A. S., David, A., Li, X., & Mehdipour, F. (2019, August). **AgentPi: An IoT Enabled Motion CCTV Surveillance System**. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 454-458). IEEE.
13. Lee, Y. S., & Kim, S. H. (2019). **A proposal of novel design on the WAVE MAC algorithm with low-latency for seamless video surveillance in V2X environment. Multimedia Tools and Applications**, 1-15.
14. Chowdhery, A., Bahl, P., & Zhang, T. (2020). **U.S. Patent No. 10,616,465**. Washington, DC: U.S. Patent and Trademark Office.
15. Mariappan, M., Thong, L. K., & Muthukaruppan, K. (2020). **A Design Methodology of an Embedded Motion-Detecting Video Surveillance System**. International Journal of Integrated Engineering, 12(2), 55-69.
16. Jin, Y., Qian, Z., & Yang, W. (2020). **UAV Cluster-Based Video Surveillance System Optimization in Heterogeneous Communication of Smart Cities**. IEEE Access, 8, 55654-55664.
17. Naim, M. H., Mohayat, J. M. Z., Abd Jalil, K., Ph'ng, L. M., Salahuddin, L., Hamid, M. H. A., & Basiron, H. (2020). **An Analysis of Standardized Data for Fog Computing Storage Capacity using Non-Relational Database**. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3). https://doi.org/10.30534/ijatcse/2020/0791.32020
18. Wang, H. (2019, November). **Edge Computing-Enabled Resource Provisioning for Video Surveillance in Internet of Vehicles**. In Smart City and Informatization: 7th International Conference, iSCI

2019, Guangzhou, China, November 12–15, 2019, Proceedings (Vol. 1122, p. 128). Springer Nature.

19. Alsmirat, M. A., Jararweh, Y., Obaidat, I., & Gupta, B. B. (2017). **Internet of surveillance: a cloud supported large-scale wireless surveillance system**. The Journal of Supercomputing, 73(3), 973-992. https://doi.org/10.1007/s11227-016-1857-x
20. Venkat, A., KP, G. V., & Thomas, I. S. (2020). **Machine Learning Based Analysis for Road Accident Prediction**. Machine Learning Based Analysis for Road Accident Prediction (March 7, 2020). IJETIE, 6(2).
21. Pandey, I. R., Raj, M., Sah, K. K., Mathew, T.,& Padmini, M. S. (2019). **Face Recognition Using Machine Learning**.
22. Chokkadi, S., &Bhandary, A. (2019). **A study on various state of the art of the art face recognition system using deep learning techniques**. arXiv preprint arXiv:1911.08426.*DOI: 10.30534/ijatcse/2019/84842019*
23. Sun, J., Shao, J., & He, C. (2019). **Abnormal event detection for video surveillance using deep one-class learning. Multimedia Tools and Applications**, 78(3), 3633-3647.
24. Lumaban, M. B. P., &Battung, G. T. (2020). **CCTV-Based Surveillance System with Face Recognition Feature**. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3). https://doi.org/10.30534/ijatcse/2020/5491.32020
25. Gayathri, M., Meghana, M., Trivedh, M., & Manju, D. (2020). **Suspicious Activity Detection and Tracking through Unmanned Aerial Vehicle Using Deep Learning Techniques**. International Journal of Advanced Trends in Computer Science and Engineering, 9(3).