IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Real-Time Anomaly Detection Surveillance System

Nayan Tuteja Department of Computer Science and Engineering Delhi Technical Campus, Uttar Pradesh, India

Hemant Department of Computer Science and Engineering Delhi Technical Campus, Uttar Pradesh, India

Chhabil Nagar Department of Computer Science and Engineering Delhi Technical Campus, Uttar Pradesh, India

Nakul Kaushik Department of Computer Science and Engineering Delhi Technical Campus, Uttar Pradesh, India

Rachna Sharma Department of Computer Science and Engineering Delhi Technical Campus, Uttar Pradesh, India

Abstract— Today's age put a significant amount of emphasis on monitoring systems. It has received a lot of research recently due to its connection to picture understanding and video analysis. More effective tools that can extract high information content are introduced into the system when artificial intelligence, deep learning, and machine learning are integrated to address the issues with standard style. Most anomaly detection tools focus on indoor surveillance and activity monitoring, which help identify abnormal behavior by watching the live stream footage. The most important of them all is the detection of human nature. It is the most strange behavior, which makes it difficult to assess whether it is normal or suspicious. This study demonstrates how in-depth learning can be used to spot odd behaviour on college or high school campuses. Employing consecutive camera frames obtained from a video, the monitoring is done. We will use our model to find the abnormal behaviour in the extracted camera frames. As soon as an anomaly is found, the stream is saved, alerting the relevant people. Therefore, we only need to save the portion of the video where the anomaly is occurring, rather than recording the entire feed. The system is composed of two parts. In the first section, features will be computed from the live video stream, and the classifier will use those features to forecast the anomaly in the second section. The proposed system can recognize the anomalies with a loss of 4.795.

Keywords— ***LSTM, CNN, Autoencoders, Reconstruction error, Regularity Score***

I. Introduction

As of 2016, there were over 350 million surveillance cameras in use worldwide. According to estimates, this number will increase to close to 1 billion by 2021. The repetitive and mistake nature of all other tiny and simple surveillance systems requires human staff to regularly examine a large number of feeds or camera footage. In comparison, some developed countries deploy sophisticated surveillance methods including huge camera networks and artificial intelligence systems. These camera feeds might possibly be automatically examined, which might reduce as well as reduce the reliance on people to repair errors made by these systems. The object of this project is to create a robust, living person surveillance system for a campus that can identify unusual behavior there and notify the relevant people.

There are numerous uses for behavioural detection [1], particularly in indoor and outdoor environments. As security cameras grow more prevalent, e-surveillance rises to importance in modern India. Effective monitoring, cost-effectiveness, and a reduced in need of people are some of its advantages. Humans now perform monitoring, which requires a significant amount of time and storage areas for the video. Automation in video surveillance offers a solution to this issue [2]. Only when the anomaly is detected will the video start to be recorded and saved to the database. The issue of space and staff needs is addressed in this way. In fact, it makes it simpler to locate the exact event rather than having to view all of the camera footage.

The objectives are :

- • Developing a model with multiple [3, 4, 5, 6] convolutional, LSTM layers to track human activity on campus and detect any suspicious activity, such as drinking, smoking, or fighting, and to send out alerts when it occurs.
- Model training using [7, 8, 9] LSTM [11] architectural style deep learning networks.
- In the event that the model detects any suspicious activity, setting up an alert system [12] utilising an ESP32 microcontroller.

After a thorough Literature Review and assessment of the research gaps, the paper then goes on to describe the approach employed by us to carry out the aforementioned task of identifying suspicious human behaviour. Each strategy in the process, which employs both a supervised and an unsupervised approach, uses a different dataset. The created model's results are then given, as well as any outcome variables.
discussions, which also include new footage from training sets and model accuracy results. The authors conclude with a section that

gives a summary of the paper and ends with references.

II. Literature Review

Various problem statements, such bank frauds, [13] video surveillance, etc., can be used to detect the anomaly. The define objectives of this essay is video surveillance anomaly detection. Considering certain papers from more recent years for our literature review, there have been various studies about detecting anomalies in [14] CCTV videos.

In 2002 [15], a novel research was published in which the researchers provided a model that differentiated between normal and anomalous behavior in order to detect all normal activities and then detect abnormalities in video surveillance. They did this using the Hidden Markov Model. The same kind of process is used in this paper, however different techniques are used.

An innovative approach for training the framework to identify movement patterns and object sizes in static video surveillance was presented in 2008 [16] by a team of researchers. The novel approach involves the modelling of object speed and size to pixel level probability density functions (pdfs), which is used for modelling past data. Using a multivariate Gaussian mixture model, the pdfs of motion of the item at that location are modelled. After the implementation of this tracking technique, each GMM learns to use an EM-based approach using the output of the teaching method (unsupervised learning). To solve the limitations of the bulk of object path modelling methods, they develop this pdf technique.

The same year, [17] another paper was published in which the author offers an unsupervised technique for clustering normal vessel traffic patterns and applies it to the detection of abnormalities in sea surveillance. The Expectation-Maximization (EM) algorithm is utilised for clustering, and, similar to earlier research in GMM. Real maritime traffic videos are included in the training dataset. A more complex model for complex object detection has not yet been proposed, but his suggested model has the capability to recognize moving objects in other domains too though.

A novel approach [18] was tried to introduce in 2010, and it is divided into three parts: a dense motion field and motion statistics method in the first part, an SVM classifier for one-class classification in the second part, and PCA (principal component analysis) in the third part for feature dimensionality reduction in the last part. Their major goal is to take a surveillance video, reduce the dimensionality of its features, and then use SVM to predict the class of the video. Researchers say that this method has very low false alarm rates when it comes to detecting surveillance anomalies, and it also works admirably in complex situations where the bulk of tracking and detection modules fail.

Further research in this area brought us to a 2012 work [19] that presented a review paper that gave an overview from several recent research approaches for automated surveillance's problem of anomaly detection. Their main plan percent yield raw information from various sensors and submitting it to a feature extractor (low-level feature extractor). Following all of this preprocessing, they utilise three distinct techniques to find anomalous behavior in videos: I supervised approach; (ii) unsupervised approach; and (iii) use of a prior model.

When it comes to this specific topic, LSTMs are the researchers' first choice [20]. In 2016, another study was released in which the researchers used the LSTM, but this time, they did so in the form of multi-scale, which generated more accuracy than any conventional machine learning models. This model has been able to achieve the best accuracy potential of 99.5%.

[22] Now, have a look at some recent studies. [21] In 2018, research was published that offered an alternative to annotating films. They used multiple instances learning (MIL) to automatically discover how to forecast high anomaly detection accuracy scores.They thought of the films as bags, with normal videos acting as one bag and anomalous videos as another. Along with their research, they also generated a sizable dataset with 128 hours of films and 13 activities that can be categorized as abnormalities, such as mishaps, break-ins, and so forth. [23] In 2019, a study based on coding was printed. For results, many different techniques have been used, such as parallel computing, and a new algorithm known as ISTA (Iterative hard-thresholding algorithm) was developed for learning sparse representation and reference books. This sparse coding-based anomaly detection also used the LSTM model.

[23] A paper describing a hybrid approach that utilizes a pre-trained CNN model and a bi-directional LSTM model was published in 2020. The CNN model extracts information from both space and time, and the Bi-LSTM model is used to spot persistent aberrant behaviour. The most recent findings revealed an increase in accuracy of 3.41% and 8.09%.

[24] All of the above studies show various approaches for anomaly detection. It is discovered that there is a novel method in which it is impossible to annotate the film clips, and many studies consist of more techniques, which are capable of producing superior results than the conventional techniques. The study starts with deep learning methods but tries to include other methods and ensemble them to create better results. The paper tries to include as many things as possible for a better end.

2.1 Research Gaps

As you can see, recent research articles are taken into consideration. After carefully reading each one, it is found that the majority of studies only consider the unsupervised approach, and that there are very few studies that consider the supervised strategy. Furthermore, [24] 1-2 papers on supervised approaches were found, but they can only do one-class classification, in comparison to unsupervised approaches, which can do multi-class classification.

III. METHODS

In our proposed system, the video from the CCTV cameras placed around the school is utilised. Our model examines the video, detects abnormalities, forecasts them, and generates the message in response. Three elements balance out the methodology: Perception: To ensure that the campus is completely covered and that the models have a constant supply of data to process, regular wireless cameras have been put around [25]. These cameras use radio waves to wirelessly deliver video feeds. Transmission: A wireless local area network [26] can be erected over the campus's wired network to enable the reception of the video signals sent by the wireless cameras.

These video signals are processed, and the frames of the video are temporarily held for the processing layers to work on it before being saved or discarded based on the nature of the processing's output. Processing: These models' output show whether the footage contains abnormal behavior or activities. The authority is either alerted or not, depending on the prediction.

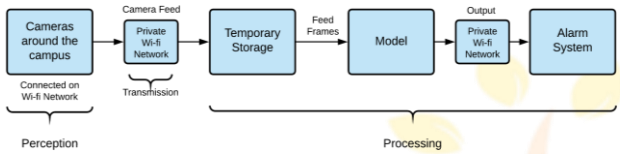

Fig 1. Methodology

These models are made using a variety of techniques, including Convolution, Carpooling, Input, Flatten, and Dense layers make up our model's layers, each of which carries out a distinct function from the others. Both direct and indirect combination enables between each layer. rely and SoftMax activation functions with a dropout rate of 0.5 are also included in the model. Finally, Adam optimizer with learning rate of 0.01 and categorical cross-entropy loss function are utilised in its development. The layers that are present and how they relate to one another are shown in Figure 1.

3.1 Dataset

The UCSD anomaly dataset [27, 28] will be utilized. The clips were taken with such a stationary camera that recorded 200 frames of a pedestrian walkway. Bikers, skateboarders, carts, and people walking in the grass around it are frequent anomalies seen in these movies. When seen, these oddities happened that way. The dataset was divided into two sets, each reflecting a different scene. These video frames are divided into 10-second temporal sequences, then the images are scaled to 256x256.

The Autoencoders use these already processed images as inputs as they attempt to reconstruct [29] these sequences and update themselves accordingly.

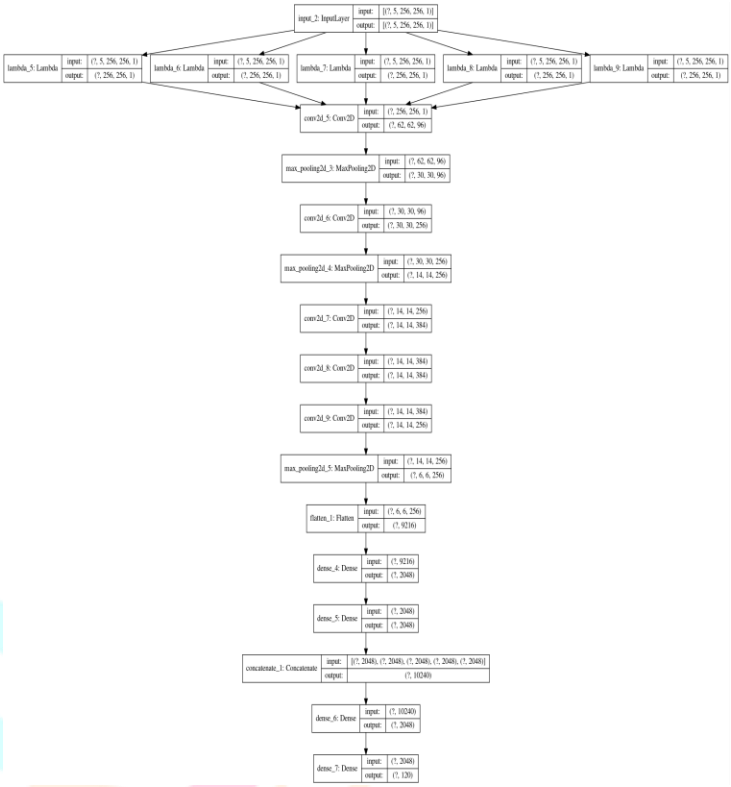

Fig 2. Information about the relationships between the model layers.

Below is figure 2, which represents how the training took place.

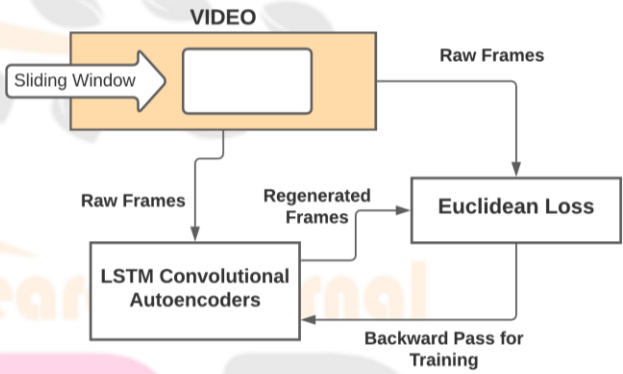

Fig 3. Algorithm applied for the training

3.2 Alarm System

The ESP32 microcontroller is being used to build an alarm system. A piezo buzzer on it may produce standard beeps and tones. A MOSFET swap siren with a high wattage can be utilised if a loud alarm is necessary. For the ESP32 and Python script to communicate, socket communication is necessary. It is simple to implement if Python's socket module is used. For this to work, the ESP32 has to be aware of the IP address of the machine and the port number of the socket it created in Python.

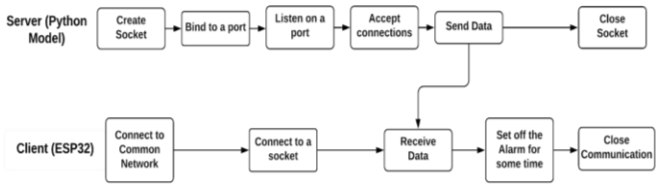

Fig 4: Socket Communication FlowChart

Because the alarm requires a working 24/7 Wi-Fi connection to receive the data and trigger the alert, FreeRTOS is used to build a task on the ESP32 that checks the Wi-Fi connection every 10 seconds. The FreeRTOS operating system kernel is part of the Espressif Internet Development Framework (ESP-IDF), which is usually used to build the ESP32 microcontroller.

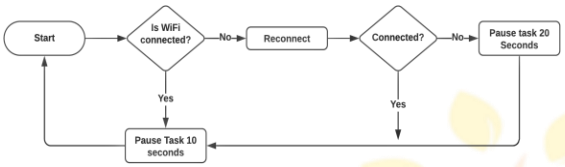

Fig 5: FlowChart of FreeRTOS task

3.3 Future Scope

3.3.1 Supervised approach

This approach classifies the anomaly (if present) into one of these 3 categories:

1. Assault
2. Using Mobile Phones
3. Firearms

3.3.2 Dataset

We used the KTH dataset [30], a well used action recognition dataset, for supervised learning. Running, walking, hand-waving, clapping, jogging, and boxing are six of the human movements included in this dataset. In addition to jogging and boxing, other activities are employed to prepare the model for routine or low-risk tasks.

The above tasks were carried out by 25 subjects in 4 scenarios: outdoors, outside with scale variation, inside, as well as outside with various clothes. There are currently 600 films in total, each of which was recorded at a frame rate of 25. We will employ the CAVIAR [31] dataset to train the model for questionable activity. The recorded movies were shot in a Lisbon retail area and the INRIA Labs' lobby entrance. Each movie has a 384x288 pixel resolution and 25 frames per second. Each video has a file size of between 6 and 12 MB, with a couple reaching 21 MB. Following the gathering of video data, each movie is preprocessed by splitting it into 7000 individual image frames. The OpenCV package was used to resize these photos to 224x224x3 pixels.

The figure illustrates the commonly used deep network model VGG16 [32]. The network consists of sixteen layers in total, with 3x3 and 1x1 convolutional layers with ReLu activation, 2x2 max pooling, and 3 fully connected layers with 4096, 4096, and 1000 units each. The fully connected layers are not used for feature extraction; rather, pre-trained convolutional and max-pooling layers are employed. After being extracted, the features are fed into LSTM [33] networks, which are Utilise with capacity to recall information and identify patterns.

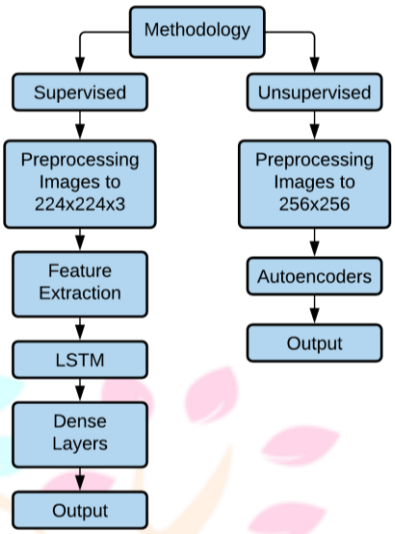

Fig 5. The workflow in Supervised and Unsupervised

3.3.3 Unsupervised approach

Since abnormal events are so rare and varied, supervised learning often leads to biassed models and poor outcomes. Realistic outcomes are achieved when unsupervised or semi-supervised learning is used to unlabeled photos. One of the many unsupervised learning methods used to identify regularities and patterns in the input data is autoencoding.

IV. Result & Discussion

This article utilizes the [34, 35, 36, 37] technique. Convolutional LSTM (38, 39, 40, 41) Using an autoencoder model on the UCSD anomaly dataset, we trained the model with three epochs, each of which contains fifty sub-steps, and four batch. The method we used is unsupervised; we did not use supervised methods because these require labelled data, and gathering labelled data for anomaly is challenging because these activities are exceptionally rare, have a wide variety of types, and will require a lot more time to label. These are the significant obstacles to the use of supervised approaches. Unsupervised and semi-supervised techniques can also be used, but they only need video evidence of anomalous activities that is readily available in the real world.

The primary tactic emphasizes on the reconstruction error; to use this strategy, we train the autoencoder first, which will allow it to rebuild only regular videos with minimum errors. Figure 6 is shown below, and it offers a thorough description of the algorithm accountable for the reconstruction error.

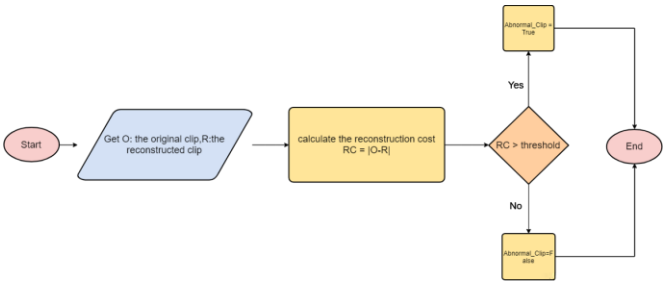

Fig 6. Algorithm explaining the concept of Reconstruction error

Using the L2 Norm, the reconstruction error of a pixel's intensity value I at the coordinates (x,y) in frame t of video:

$$e(x,y,t) = ||I(x,y,t) - f_w(I(x,y,t))||_2 \quad (1)$$

Here, f_w is the learned LSTM convolutional encode, the reconstruction error of frame t is calculated by summing up all the pixel's error:

$$e(t) = \sum_{(x,y)} e(x,y,t) \quad (2)$$

Let's suppose we have to find out reconstruction cost which is starting at t can be calculated as:

$$SequenceReconstructionCost(t) = \sum_{t'=t}^{t+10} e(t') \quad (3)$$

Now, the abnormality score is calculated:

$$s_a(t) = \frac{SequenceReconstructionCost(t) - SequenceReconstructionCost(t)}{SequenceReconstructionCost(t)_{max}} \quad (4)$$

After this regularity score is calculated for the plotting of graph and finding the abnormal events:

$$s_r(t) = 1 - s_a(t) \quad (5)$$

To guarantee that the input photos have the same resolution as the video frames, each video frame is resized to 256x256 by dividing the pixel size between 0 and 1. After training is complete, the by some 4.795 and the validation loss equals 4.7935. Figure 7 is a sample clip from the dataset that is given.

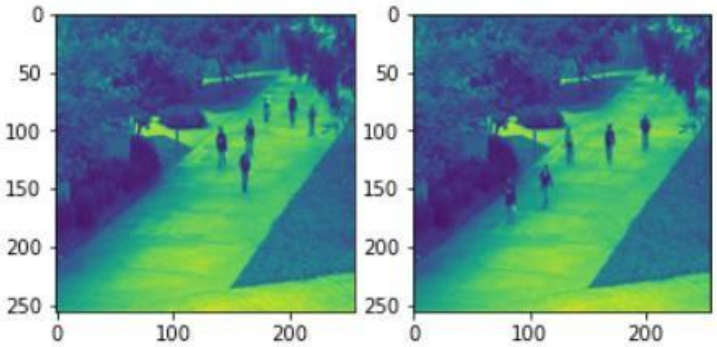

Fig 7. Clips from the training set

The autoencoder is composed of an encoder and a decoder. The encoder accepts the input video as a series of frames, and it is comprised of two elements: a spatial encoder for features and a temporal encoder for motion.

For the purpose of obtaining the results, the model is applied to a test set in which a video is selected for the model's testing and each clip of that video is then converted into tensors, which reflect the activity happening in the testing video. The current activity is represented by tensors in Figure 8 below with regard to time.

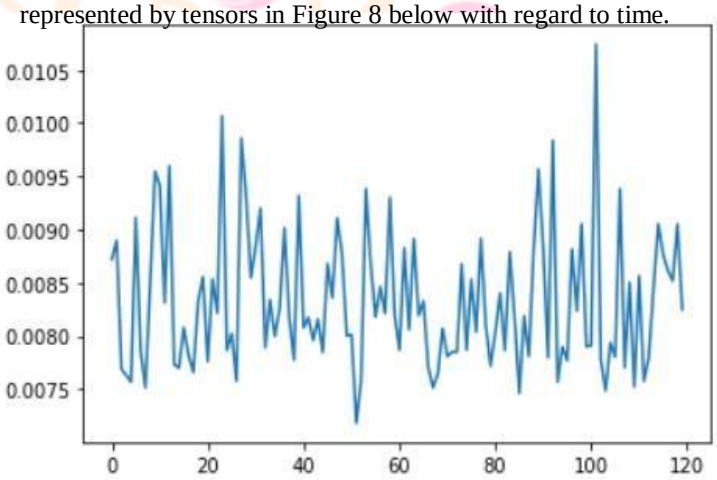

Fig 8. Representation of activities in the form of tensors, the x-axis is the time and y-axis are tensors

As a result of completely connected LSTM layers' inability to maintain their data due to their entire connections, convolutional LSTM is used in this model in place of fully connected LSTM layers.

Now, using the regularity score, an anomaly is found. Figure 9 below is an example of an anomaly that was found using the regularity rating of just one test video.

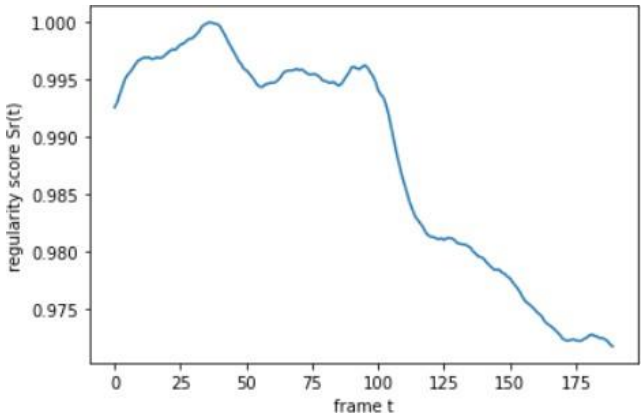

Fig 9. Detection of Abnormal activity through regularity score

In this chart, a high regularity scores indicate that there are no aberrant or anomalous responses in the frame at that time, while a low regularity score means there seem to be anomalous or abnormal tendencies in the frame at that time.

V. CONCLUSION

This study's main goal is to identify any anomalies that may be occurring in the real world. Convolutional LSTM autoencoders model is an unsupervised method that we used to achieve this. Finally, we discovered a technique in autoencoders called regularity score that modifies along with the behaviour of the particular scene or video. The suggested study will be used for academic purposes in order to spot any anomalies occurring in the academic setting.

This paper reports the successful application of anomaly detection on the UCSD anomaly detection dataset with a loss of about 4.7. This study will make it easier to spot other anomalies in our surroundings.

VI. REFERENCES

[1] Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020).

[2] 2. G. Sreenu and M. A. Saleem Durai "Intelligent video surveillance: a review through deep learning techniques for crowd analysis", *Journal Big Data,2019.*

[3] 3. Kim, Tae-Young, and Sung-Bae Cho. "Web traffic anomaly detection using C-LSTM neural networks." *Expert Systems with Applications 2018.*

[4] 4. Feng, Fang, et al. "Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device." *Ad Hoc Networks* 84 (2019): 82-89.

[5] 5. Khan, Muhammad Ashfaq, Md Karim, and Yangwoo Kim. "A scalable and hybrid intrusion detection system based on the convolutional-LSTM network." *Symmetry* 11.4 (2019): 583.

[6] 6. Cao, Kerang, et al. "CNN-LSTM coupled model for prediction of waterworks operation data." *Journal of Information Processing Systems* 14.6 (2018): 1508-1520.

[7] 7. Zhong, Zhi, et al. "A deep learning approach to anomaly detection in geological carbon sequestration sites using pressure measurements." *Journal of hydrology* 573 (2019): 885-894.

[8] 8. Xie, Guo, et al. "Motion trajectory prediction based on a CNN-LSTM sequential model." *Science China Information Sciences* 63.11 (2020): 1-21.

[9] 9. Naseer, Sheraz, et al. "Enhanced network anomaly detection based on deep neural networks." *IEEE Access* 6 (2018): 48231-48246.

[10] 10. Chalapathy, Raghavendra, and Sanjay Chawla. "Deep learning for anomaly detection: A survey." *arXiv preprint arXiv:1901.03407* (2019).

[11] 11. Javier Abellan-Abenza, Alberto Garcia-Garcia, Sergiu Oprea, David Ivorra-Piqueres, Jose Garcia-Rodriguez "Classifying Behaviours in Videos with Recurrent Neural Networks", *International Journal of Computer Vision and Image Processing, December 2017.*

[12] 12. Liu, Yi, et al. "Deep Anomaly Detection for Time-series Data in Industrial IoT: A Communication-Efficient On-device Federated Learning Approach." *IEEE Internet of Things Journal* (2020).

[13] 13. Kumaran, Santhosh Kelathodi, Debi Prosad Dogra, and Partha Pratim Roy. "Anomaly detection in road traffic using visual surveillance: A survey." *arXiv preprint arXiv:1901.08292* (2019).

[14] 14. Hu, Weiming, et al. "A survey on visual surveillance of object motion and behaviors." *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 34.3 (2004): 334-352.

[15] 15. Clark, Vinod Nair James J. "Automated visual surveillance using hidden markov models." *International Conference on Vision Interface*. 2002.

[16] 16. Arslan Basharat, Alexei Gritai, Mubarak Shah. "Learning object motion patterns for anomaly detection and improved object detection". *IEEE Conference on Computer Vision and Pattern Recognition 2008.*

[17] 17. Rikard Laxhammar. "Anomaly detection for sea surveillance". *11th International Conference on Information Fusion 2008.*

[18] 18. Chang Liu, Guijin Wang, Wenxin Ning, Xinggan Lin, Lian Zi, Zhou Liu. "Anomaly detection in surveillance video using motion direction statistics". *IEEE International Conference on Image Processing. 2010.*

[19] 19. Angela A. Sodemann, Matthew P. Ross, Brett J. Borghetti. "A Review of Anomaly Detection in Automated Surveillance". *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 2012.*

[20] 20. M. Cheng, Q. Xu, J. L.V., W. Liu, Q. Li and J. Wang, "MS-LSTM: A multi-scale LSTM model for BGP anomaly detection," *2016 IEEE 24th International Conference on Network Protocols (ICNP)*, Singapore, 2016.

[21] 21. P.Bhagya Divya, S.Shalini, R.Deepa, Baddeli Sravya Reddy, "Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras", *International Research Journal of Engineering and Technology (IRJET), December 2017.*

[22] 22. J. T. Zhou, J. Du, H. Zhu, X. Peng, Y. Liu and R. S. M. Goh, "AnomalyNet: An Anomaly Detection Network for Video Surveillance," in *IEEE Transactions on Information Forensics and Security 2019.*

[23] 23. Ullah, Waseem, et al. "CNN features with bi-directional LSTM for real-time anomaly detection in surveillance networks." *Multimedia Tools and Applications* (2020).

[24] 24. Kiran, B. Ravi, Dilip Mathew Thomas, and Ranjith Parakkal. "An overview of deep learning based methods for unsupervised and semi- supervised anomaly detection in videos." *Journal of Imaging* 4.2 (2018): 36.

[25] 25. Zhiqing Zhou, Heng Yu, Hesheng Shi, "Optimization of Wireless Video Surveillance System for Smart Campus Based on Internet of Things", *IEEE Access, Vol. 8, pp. 136434–136448, 2020.*

[26] 26. Yin, Chunyong, et al. "Anomaly Detection Based on Convolutional Recurrent Autoencoder for IoT Time Series." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (2020).

[27] 27.UCSD Anomaly Detection Dataset(http://svcl.ucsd.edu/projects/anomaly/dataset.htm).

[28] 28. A. Khaleghi and M. S. Moin, "Improved anomaly detection in surveillance videos based on a deep learning method," *2018 8th Conference of AI & Robotics and 10th RoboCup Iranopen International Symposium (IRANOPEN) 2018.*

[29] 29. Yufan Zhou, Haiwei Dong, Abdulmotaleb El Saddik, "Deep Learning in Next-Frame Prediction: A Benchmark Review", *IEEE Access, Vol. 8, pp. 69273–69283, 2020.*

[30] 30. Christian Schuldt, Ivan Laptev and Barbara Caputo, "Recognizing Human Actions: A Local SVM Approach" *Proc. ICPR'04, Cambridge, UK.*

[31] 31. Oliver Brdiczka, Jerome Maisonnasse, Patrick Reignier, "Automatic Detection of Interaction Groups", *ICMI '05, 2005 International Conference on Multimodal Interaction, Trento, Italy, October 2005.*

[32] 32. Karen Simonyan, Andrew Zisserman," Very Deep Convolutional Networks for Large-Scale Image Recognition", *ICLR 2015.*

[33] 33. S. Hochreiter and J. Schmidhuber, "Long short-term memory", *Neural Comput., vol. 9, no. 8, pp. 1735-1780, 1997.*

[34] 34. W. Luo, W. Liu and S. Gao, "Remembering history with convolutional LSTM for anomaly detection," *2017 IEEE International Conference on Multimedia and Expo (ICME)*, Hong Kong, 2017.

[35] 35. Javed, Abdul Rehman, et al. "Anomaly detection in automated vehicles using multistage attention-based convolutional neural network." *IEEE Transactions on Intelligent Transportation Systems* (2020).

[36] 36. Heryadi, Yaya, and Harco Leslie Hendric Spits Warnars. "Learning temporal representation of transaction amount for fraudulent transaction recognition using cnn, stacked lstm, and cnn- lstm." *2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom)*. IEEE, 2017.

[37] 37. Swapna, Goutham, Soman Kp, and Ravi Vinayakumar. "Automated detection of diabetes using CNN and CNN-LSTM network and heart rate signals." *Procedia computer science* 132 (2018): 1253-1262.

[38] 38. Zhao, Yiru, et al. "Spatio-temporal autoencoder for video anomaly detection." *Proceedings of the 25th ACM international conference on Multimedia*. 2017.

[39] 39. Sakurada, Mayu, and Takehisa Yairi. "Anomaly detection using autoencoders with nonlinear dimensionality reduction." *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis*. 2014.

[40] 40. Chen, Zhaomin, et al. "Autoencoder-based network anomaly detection." *2018 Wireless Telecommunications Symposium (WTS)*. IEEE, 2018.

[41] 41. Cozzolino, Davide, and Luisa Verdoliva. "Single-image splicing localization through autoencoder-based anomaly detection." *2016 IEEE international workshop on information forensics and security (WIFS)*. IEEE, 2016.