JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 10, Issue.4, April 2022 E-ISSN: 2347-2693

An Online Predictive System for Mapping Visual Scenes of Fraudulent Behaviour

C. Ubani[1*], V.I.E. Anireh[2], N.D. Nwiabu[3]

[1,2,3]Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

[*]*Corresponding Author: ubanichinyere677@gmail.com, Tel.: +2348038935662*

DOI: https://doi.org/10.26438/ijcse/v10i4.1620 | Available online at: www.ijcseonline.org

Received: 09/Mar/2022, Accepted: 11/Apr/2022, Published: 30/Apr/2022

Abstract— Fraudulent behaviour are suspicious activities that usually occur before a crime takes place. These suspicious activities are being carried out on a day-to-day basis in banks, supermarkets, restaurants, Bus stop, offices, residential buildings, companies e.t.c. Within the banking industry, fraudulent behaviour is when a customer or a person makes suspicious moves before committing a crime. In this paper, an online predictive system for mapping visual scene against fraudulent behaviour was developed. The dataset for this system was collected from Kaggle database. The analysis of the video clips gave a total of 427 frames, 380 was visually mapped to be of fraudulent behaviour while 47 was being mapped to be of normal behaviour. These frames were used in training a convolutional neural network for detecting fraudulent behaviour from a video clip. The proposed model was deployed to web using python and flask framework. Our result gave about 99.99%. The proposed system was compared with that of Nakib et.al. (2018). The result of Nakib et.al. (2018) gave an accuracy of about 90.2% while that of our proposed system gave 99.99%.

Keywords— Fraudulent Behaviour, Visual Scenes, Surveillance Camera, Deep Learning

I. INTRODUCTION

The actual surrounding has the ability to be extraordinarily within the research and determination of suspected fraudulent behaviour. Actions carried out early within crook’s investigate the crime scene are important to understanding this capacity. Nowadays, Artificial intelligence is being evolved to predict results in a certain situation in a certain situation or vicinity following patterns of a few historical data. For a framework to be predictive, predictions need to be primarily totally based on a few acknowledged styles [1]. This class of systems needs to be capable of studying from acknowledged examples, the use of their patterns and labels to study an unlabeled and unknown example [2]. There are distinctive algorithms that can be applied to expand predictive frameworks, they include neural networks, Bayesian networks, decision trees, logistic regression, and such likes [3], and they may be being hired to enhance that can be applied to the modern framework.

Fraudulent conduct is an act that includes a deviation from the regular manner of human conduct. In [4] they mentioned a Theory of Reason Action (TRA) that's defined to be targeted at the cognitive perception system, it facilitates in probing behaviours of people. These people engage with the laptop system, at some point in which facts may be accumulated and evaluated [5]. In existence, humans generally tend to have a look at various social norms whilst they may be online compared to whilst they may be offline. Whereas the net become alleged to be nameless and private, humans have more and more enriched the cyber area with private facts thereby growing the safety problems confronted by customers getting access to the net [6].

Mapping visible scenes to fraudulent conduct can either be defined as a way of understanding what mapping clearly is. Mapping is the manner of creating a map; it offers an analyst the graphical illustration of a crime place and understanding of the place and the motives by which such crimes occur. In crime mapping, it's miles the usage of the geographical facts system (GIS) to carry out a spatial evaluation of crime hassle that pertains to police investigations [7]. In computing, it's miles the era utilized by regulation enforcement organizations within the evaluation and correlation of information sources, developing an in-depth snapshot of crime incidents and elements associated with those crimes inside a geographical place or community [8]. So, in mapping visible scenes, one has to be capable of constituting visible evidence/ clues in a map; however, digitally (that is, online). The virtual footprints that are the feature of the fraudulent behavior of the criminals are represented on a map and are used to expect a criminal offense or fraudulent acts online. Hence, a web-based predictive set of rules may be evolved for mapping visible scenes to fraudulent behaviour the use of the sort of synthetic intelligence strategies specifically within the diverse e-commerce frameworks bobbing up in the latest times.

II. RELATED WORK

[9] implemented CNN in crime scene prediction through detecting threatening gadgets. Without human assistance,

crime scene prediction will have a giant effect on laptop's imagination and prescient. The utilization of CNN (Convolutional Neural Network) to discover knives, blood, and gun from a photo is provided in this study. Detecting those dangerous gadgets in a photo can assist us to decide whether or not or now no longer a criminal offense has come about, in addition to wherein the photo became captured. We targeted detecting accuracy in order that we do not get fake indicators and may make the maximum of the machine. To arrive at a detection end result, this version employs the Rectified Linear Unit (ReLU), Convolutional Layer, Fully Connected Layer, and CNN dropout characteristic. To reap our favored effects, we broaden CNN the usage of TensorFlow, an open supply platform. For the examined dataset, the cautioned version obtains 90.2 percent accuracy.

[10] evaluated different areas of corruption with varying degrees of significance using data mining tools developed by various researchers to promote reducing crime rates by discovering, diminishing, or preventing violence. emerging. At different stages of data mining methodologies were also used. Information gathering, analysis, and model creation are all part of the process. The use of previously collected data. The use of knowledge to boost expectations in crime prevention is an area where further research is needed inspection because it has the potential to save lives and prevent calamities

[11] used open data from police reports, assess the effectiveness of deep learning algorithms in this domain, and make recommendations for constructing and training deep learning systems for predicting crime regions. A comparison analysis of 10 state-of-the-art approaches against three alternative deep learning configurations is completed using a time series of crime types per location as training data. The result of the authors shows that deep learning-based algorithms routinely beat previous best-performing methods in their experiments using five publicly available datasets. Furthermore, they assess the efficacy of various parameters in deep learning architectures and provide recommendations for setting them to improve crime classification and prediction performance.

[12] used a new video data set collected in low-stakes situations, test the ability of different feature sets (i.e., improved dense trajectories, OpenFace) and machine learning approaches (i.e., support vector machines vs. deep neural networks) to differentiate deception from evidence based on facial micro-expressions. During the interviews, a procedure was used to elevate the computational burden of the offenders, allowing for the detection of false cues. The best performing method was support vector machines (SVMs) combined with OpenFace (AUC = 0.72 videos without cognitive load; AUC = 0.78 movies with cognitive stress), according to their findings.

[13] proposed a progressive matching approach was used to detect suspicious activity in city parks. Adjacency matrix-based classification and support vector machines are used for a heterogeneous crowd to spot abnormal and abnormal activities. The work of object detection and tracking will be enhanced, as well as all components of activity identification in a human swarm of people in public places. The support vector machine (SVM) is used to recognize aberrant occurrences in a crowd scenario and to vector those events to drive or limit planned actions.

In an Internet of Things (IoT) scenario, a unique deep learning-based strategy for forecasting the likelihood of anomalous occurrences using footprints obtained from networked surveillance devices and alerting users of such activities. Dynamic motion detection algorithms are used to transform captured images into still blocks and de-blur them. Then, using random forest evolutionary algorithms with kernel density (RFKD), aberrant behaviours are anticipated, and any abnormal actions detected result in signals being conveyed to IoT devices via the MQTT protocol. Deep neural network with multi-classifiers network, and kernel density functions were included in the suggested research. For input classifications from a video series of frames, the multi-classifier is utilized [14].

[15]. proposes a smart surveillance cameras system for detecting unusual human behaviour in an educational setting that takes security and emergency considerations into account by focusing on three aberrant activities (falling, boxing, and waving). This approach consists of two key processes: the first is a tracking system that can track targets and identify sets of attributes in order to fully explain the human activity and acquire descriptive data on each target. The second is a decision-making system that can determine if the activity of the target track is "normal" or "abnormal," and then activate an alarm when abnormal behaviours are detected.

Deep learning algorithms for video-based abnormal activity detection were investigated. The study produced a schematic classification for detecting abnormal events depending on different types of anomalies, the level of outlier detection, and the anomaly measurement. Various anomaly detection approaches that use deep learning techniques as their main methodology have been highlighted. Deep learning algorithms are examined from both the accuracy-oriented and real-time processing-oriented aspects of anomaly detection [16].

III. METHODOLOGY

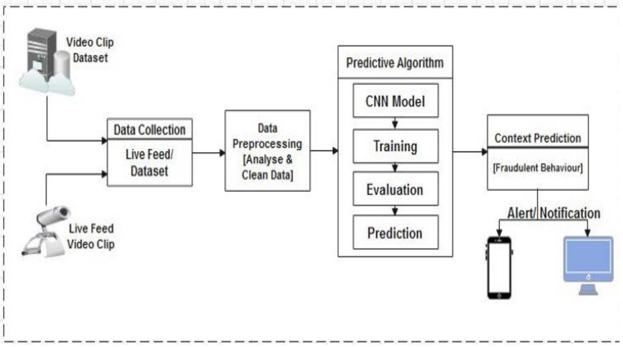


Figure 1: Architecture of the System

Figure 1 is an illustration of the proposed online predictive algorithm for mapping visual scenes to fraudulent behaviour. Data is being collected from either a video clip dataset or live feed from a video camera. The dataset is used to train the model which will be during the development stage and the live feed is collected during the implementation of the system. the data collected if analyzed and cleaned for use by the predictive algorithm (CNN model) after which a context prediction is carried out. When fraudulent behaviour is detected, an online notification is then sent to the appropriate security personnel on their mobile device or the computer system for preventive and/ or proactive action to be taken.

A. Data Collection

The data for the proposed system is collected via the dataset or the camera feed and its fed into the system for analysis and cleaning. This data is collected almost the way an image data is collected and processed.

B. Data Pre-processing

The pre-processing of the video data is done on frame bases. Each frame of the video clip is collected resized and analysed to be able to track the frames and the behaviour exhibited on each videos clip.

C. Predictive Algorithm

The convolutional neural network (CNN) model has been adopted as the predictive algorithm for this research work. The model has been used for several machine learning video classification and has been chosen as a prediction algorithm for the mapping of visual scene to fraudulent behaviour. The schema that illustrates the CNN working principle is shown in Figure2

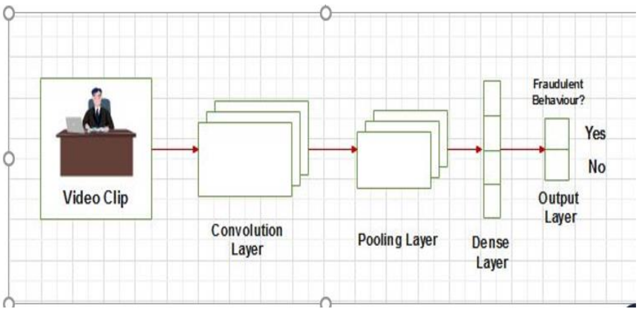


Figure 2: Convolutional Neural Network Framework for the Proposed System

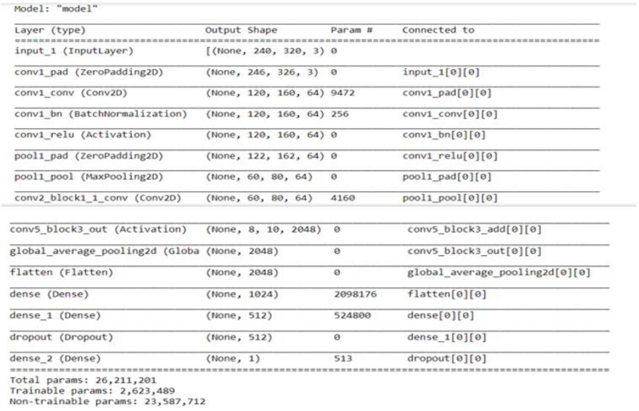
Figure 3.2 is a convolutional neural network framework of the proposed system explaining the working process to the output of the system. The video data is passed to the convolutional layer through the input layer. This is the core building block of the convolutional network. The convolution layer helps to abstract the features to a map; it convolves the video input and pass the result the next layer, which is the pooling layer. The pooling layer is responsible with the reduction of data dimensions as it combines the output of neuron clusters in one layer to a single neuron in the next layer. The dense layer is also known as the fully connected layer which describes the connectivity that exist in the next layer after which, we have the output layer which presents the result of a fraudulent behaviour or not.

D. Context Prediction

The context prediction simply displays classification or prediction of the context of the video being analyzed. This output is displayed after it has gone through the CNN model that was trained and evaluated. It tells whether the behavior portrayed by the subject(s) is fraudulent and can predict accordingly. When fraudulent behavior is detected, an alert/ notification is sent accordingly for proactive or preventive measures.

IV. RESULTS AND DISCUSSION

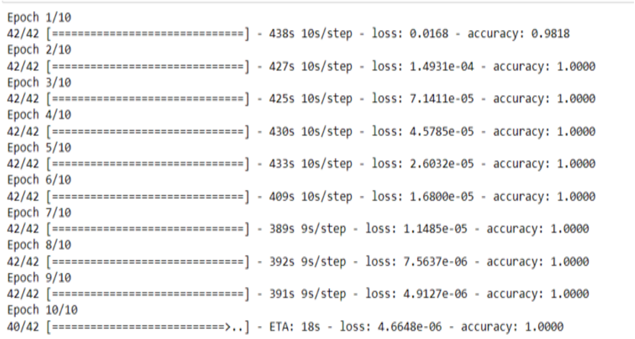
This system presents a smart system for detecting fraudulent behaviours from video scenes. The dataset used in this work is a surveillance video comprised of the various fraudulent and normal behavior of various individuals. A total of ten different videos was downloaded from various online resources like YouTube, Dreamweaver, google. These videos are surveillance videos from supermarkets, ATMs, Bus stops, houses, etc. The downloaded videos were saved into the working directory for further pre-processing. In other to have better training data, each of the videos needs to be broken down into various frames. For this purpose, the Opencv library was used in reading the videos from the working directory and extracting different frames from the videos. For a particular video, over 427 frames were been generated. In the frames generated, 380 frames were being mapped as fraudulent behaviour while that of 40 was mapped as normal frames. This was done to have better training data. The frames generated was divided into two folders. The folders are normal and fraudulent folder. The generated frames were used in training a convolutional neural network algorithm in detecting fraudulent behaviours. The proposed model was built using images of both fraudulent and normal behavior. The images were read and pre-processed using ImageDataGenerator. This was used in reading the images from the directory as binary files (0,1). Setting 0 represent normal human behavior and setting 1 is fraudulent human behavior. The pre-processed data was trained using a convolutional neural network. The following parameters were used. Input_shape = (240, 320, 3), first layer (1024), activation = “relu”, Second layer (512), activation=”relu”, dropout=0.3 was used in reducing overfitting of the model, and finally the output layer=1, and activation=sigmoid. The model was compiled using optimizer= Adam, loss=binary_crossentropy. Epoch =10, the number of steps per epoch = length/bactch_size. The summary of the model can be seen in figure 4. The training process of the proposed model can be seen in figure 7. The training accuracy of the proposed model can be seen in figure 5, whereas the loss values obtained by the proposed system model can be seen in figure 6. The precited result on a test video can be seen in figure 7 The classification report of the model’s performance can be seen in figure 8.



```
Model: "model"
________________________________________________________________________________________________
Layer (type)                    Output Shape         Param #     Connected to
================================================================================================
input_1 (InputLayer)            [(None, 240, 320, 3) 0
________________________________________________________________________________________________
conv1_pad (ZeroPadding2D)       (None, 246, 326, 3)  0           input_1[0][0]
________________________________________________________________________________________________
conv1_conv (Conv2D)             (None, 120, 160, 64) 9472        conv1_pad[0][0]
________________________________________________________________________________________________
conv1_bn (BatchNormalization)   (None, 120, 160, 64) 256         conv1_conv[0][0]
________________________________________________________________________________________________
conv1_relu (Activation)         (None, 120, 160, 64) 0           conv1_bn[0][0]
________________________________________________________________________________________________
pool1_pad (ZeroPadding2D)       (None, 122, 162, 64) 0           conv1_relu[0][0]
________________________________________________________________________________________________
pool1_pool (MaxPooling2D)       (None, 60, 80, 64)   0           pool1_pad[0][0]
________________________________________________________________________________________________
conv2_block1_1_conv (Conv2D)    (None, 60, 80, 64)   4160        pool1_pool[0][0]

________________________________________________________________________________________________
conv5_block3_out (Activation)   (None, 8, 10, 2048)  0           conv5_block3_add[0][0]
________________________________________________________________________________________________
global_average_pooling2d (Globa (None, 2048)         0           conv5_block3_out[0][0]
________________________________________________________________________________________________
flatten (Flatten)               (None, 2048)         0           global_average_pooling2d[0][0]
________________________________________________________________________________________________
dense (Dense)                   (None, 1024)         2098176     flatten[0][0]
________________________________________________________________________________________________
dense_1 (Dense)                 (None, 512)          524800      dense[0][0]
________________________________________________________________________________________________
dropout (Dropout)               (None, 512)          0           dense_1[0][0]
________________________________________________________________________________________________
dense_2 (Dense)                 (None, 1)            513         dropout[0][0]
================================================================================================
Total params: 26,211,201
Trainable params: 2,623,489
Non-trainable params: 23,587,712
```

Figure 4: Summary of the model



```
Epoch 1/10
42/42 [==============================] - 438s 10s/step - loss: 0.0168 - accuracy: 0.9818
Epoch 2/10
42/42 [==============================] - 427s 10s/step - loss: 1.4931e-04 - accuracy: 1.0000
Epoch 3/10
42/42 [==============================] - 425s 10s/step - loss: 7.1411e-05 - accuracy: 1.0000
Epoch 4/10
42/42 [==============================] - 430s 10s/step - loss: 4.5785e-05 - accuracy: 1.0000
Epoch 5/10
42/42 [==============================] - 433s 10s/step - loss: 2.6032e-05 - accuracy: 1.0000
Epoch 6/10
42/42 [==============================] - 409s 10s/step - loss: 1.6800e-05 - accuracy: 1.0000
Epoch 7/10
42/42 [==============================] - 389s 9s/step - loss: 1.1485e-05 - accuracy: 1.0000
Epoch 8/10
42/42 [==============================] - 392s 9s/step - loss: 7.5637e-06 - accuracy: 1.0000
Epoch 9/10
42/42 [==============================] - 391s 9s/step - loss: 4.9127e-06 - accuracy: 1.0000
Epoch 10/10
40/42 [===========================>..] - ETA: 18s - loss: 4.6648e-06 - accuracy: 1.0000
```

Figure 5: Training process of the proposed Convolutional Neural Network Model.

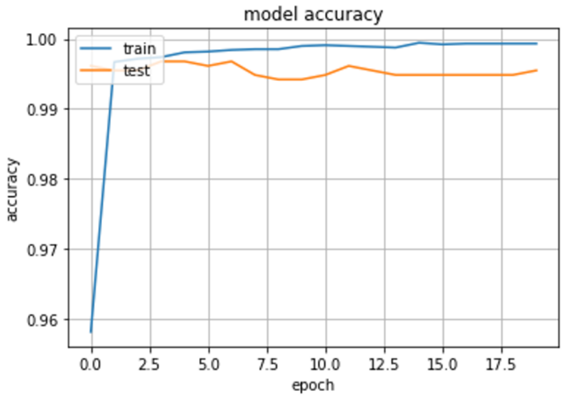


Figure 6: Training accuracy of the proposed model.

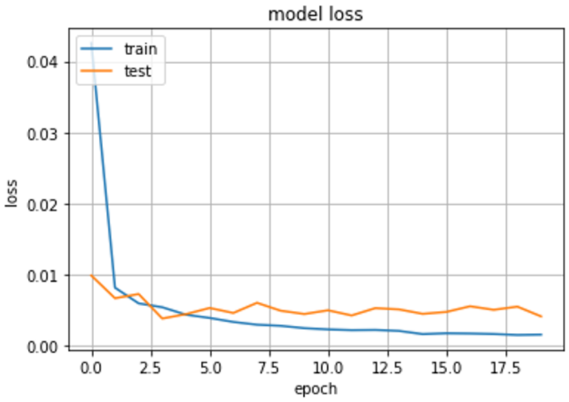
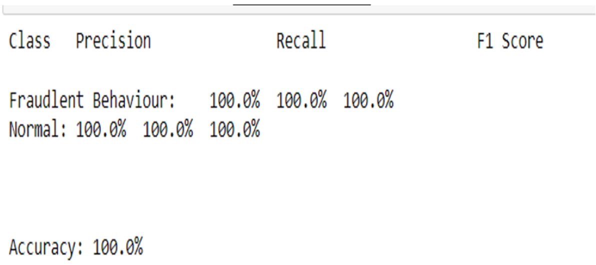


Figure 7: Model Loss



```
Class   Precision              Recall                  F1 Score

Fraudlent Behaviour:    100.0%  100.0%  100.0%
Normal: 100.0%  100.0%  100.0%



Accuracy: 100.0%
```

Figure 8: Classification Report of the Proposed Model

V. Conclusion and Future Scope

The actual surrounding has the ability to be extraordinarily vital within the research and determination of suspected fraudulent behaviour. Actions carried out early within crook research on the crime scene are important to understanding this capacity. Intelligent these days intelligent are being evolved to predict results in a given state of affairs or vicinity following styles of a few historical data. For a framework to be predictive, predictions need to be primarily totally based on a few acknowledged styles. Due to the security challenges in Nigeria and the world at large, detecting fraudulent behaviour before the scene is carried out will be a great benefit to Nigeria and the world at large. Therefore, this thesis presents an online system for detecting fraudulent behaviours on a surveillance video. The system starts by extracting frames from the video and converting them to images automatically. The system uses the extracted images in building a convolutional neural network model so as to enable it to detect and alert the user for fraudulent activities detected on a video scene. The result of the model shows that the model achieved an accuracy result of about 99.99%. The result of the proposed system was compared to an existing method. And this shows that the model outperforms the existing system**.**

References

[1]. S. Jatav, V. Sharma, "An algorithm for predictive data mining approach in medical diagnosis", International Journal of Computer Science & Information Technology (IJCSIT) **Vol, 10., 2018.**

[2]. B. E. Aguinaldo, "21st Century Learning Skills Predictive Model Using PART Algorithm", In Proceedings of the 3rd International Conference on Machine Learning and Soft Computing, **pp. 134-137, 2019.**

[3]. T. Davenport, A. Guha, D. Grewal, T. Bressgott, "How artificial intelligence will change the future of marketing", Journal of the Academy of Marketing Science, **48(1), 24-42, 2020.**

[4]. M. Zawawi, K. Jusoff, A. Rahman, "Behavioral intention for fraudulent reporting behaviour using cognitive theory". Asian Social Science, **4(7), 43-47, 2008**

[5]. W. W. Eckerson, "Predictive analytics. Extending the Value of Your Data Warehousing Investment", TDWI Best Practices Report, **1, 1-36, 2007.**

[6]. A. Grawal, J.S. Gans, A. Goldfarb, "Exploring the impact of artificial intelligence: Prediction versus judgment", Information Economics and Policy, **47, 1-6, 2018.**

[7]. A. Sell, A, "The Same Old Story: Predictive Algorithms and the Novel". tba: Journal of Art, Media, and Visual Culture, **2(1), 49-58.2020**

[8]. W.H. Smith, M. Milford, K. D. McDonald-Maier, S. Ehsan, S., "Scene Retrieval for Contextual Visual Mapping". arXiv preprint arXiv:**2102.12728, 2021**

[9]. M. Nakib, R. Khan, M. Hasan, J. Uddin, J, "Crime scene prediction by detecting threatening objects using convolutional neural network", In International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2), **pp. 1-4, 2018.** IEEE.

[10]. T. Chandrakala, S. Nirmala, K. Dharmarajan, K. Selvam K, "Development Of Crime And Fraud Prediction Using Data Mining Approaches"., International Journal of Advanced Research in Engineering and Technology (IJARET) **Vol.11, Issue 12, pp. 1450-1470, December 2020.**

[11] P. Stalidis, T. Semertzidis, P. Daras, "Examining Deep Learning Architectures for Crime Classification and Prediction", Forecasting. **3(4): 741-762, 2021.** https://doi.org/10.3390/forecast3040046.

[12] M. Merylin, M. Stéphanie, C. Scarpazza, G. Nicolò, "Detecting deception through facial expressions in a dataset of videotaped interviews: A comparison between human judges and machine learning models", Computers in Human Behaviour. **127, 2022.** https://doi.org/10.1016/j.chb.2021.107063.

[13] S. Aruljothi, K. Pavithradevi, "Detection Of Suspicious Activities In Public Areas Using Staged Matching Technique", International Journal Of Advanced Information And Communication Technology. **1(1), 140-143, 2014**

[14] G. Vallathan, A. John, C. Thirumalai, S. Mohan, G. Srivastava, "Suspicious activity detection using deep learning in secure assisted living IoT environments", The Journal of Supercomputing. doi:10.1007/s11227-020-03387-8, **2020.**

[15]. J. Ali, N. Shati, M.T. Gaata, "Abnormal activity detection in surveillance video scenes". TELKOMNIKA (Telecommunication Computing Electronics and Control), 18(5), 2447. https://doi.org/10.12928/TELKOMNIKA. V18I5.16634, **2020.**

[16]. K. Pawar, V. Attar, V., "Deep learning approaches for video-based anomalous activity detection", World Wide Web. doi:10.1007/s11280-018-0582-1

AUTHORS PROFILE

Mr. C T Lin pursed Bachelor of Science from University of Taiwan, Taiwan in 2006 and Master of Science from Osmania University in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computational Sciences, Department of Electronic and Communication, University of Taiwan, Taiwan since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013, ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.

Mr C H Lin pursed Bachelor of Science and Master of Science from University of New York, USA in year 2009. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Telecommunication, University of New York, USA since 2012. He is a member of IEEE & IEEE computer society since 2013, a life member of the ISROSET since 2013 and ACM since 2011. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, Data Mining, IoT and Computational Intelligence based education. He has 5 years of teaching experience and 4 years of Research Experience.