SECURING DOCUMENTS THROUGH BLOCKCHAIN IN CLOUD

Sahil Landge, Harshal Gadekar, Yash Khandibharad, Farhan Pathan

Sahil Landge, Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India
Harshal Gadekar, Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India
Yash Khandibharad, Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India
Farhan Pathan, Cloud Computing and Big Data, Padmashri Dr Vitthalrao Vikhe Patil Institute of Technology and engineering (polytechnic), Maharashtra, India

ABSTRACT

Blockchain technology has grown from becoming an immutable database of transactions for crypto currencies to a programmable interactive environment for creating distributed reliable applications. While, blockchain technology has been used to solve numerous problems, to our knowledge none of the previous work centered on using blockchain to build a stable and immutable science data provenance management system that automatically verifies the provenance records. In this job, we use blockchain as a medium to promote trustworthy data provenance compilation, verification and management. According to numerous researches about one million graduates passing out each year, the diploma awarding authorities are seems to be corrupted for the security credentials of student records. Due to the lack of successful storage mechanism, incidents that allow the graduation certificate to be forged also get noticed. In order to address this problem digital certificate systems are adopted even though security problems are still remain. Blockchain is one of the most recent technologies that can be used for the data protection. The irreversible property of the block chain helps to solve the problem of certificate forgery.

Keywords— *Block head formation, Blockchain creation, Terminal Key generation, Bilinear Pairing.*

INTRODUCTION

Graduation certificates and documents contain material private to the people and cannot be readily available to anyone. Hence, there is a high need for a system that can ensure that the material in such a document is original, which ensures that document has come from an authenticated source and is not false. In addition, the material in the paper should be secret so that it can only be accessed by designated individuals.

Blockchain technology is used to minimize the occurrence of certificate forgeries and ensure that the reliability, legitimacy and confidentiality of graduation certificates can be enhanced. Technologies occur in related fields, such as digital fingerprints, which are used in E-documents to provide verification, credibility, and nonrepudiation. However, for the specifications of an E-qualification certificate, it has crucial security gaps and missed functions: for example, it uses the keys to validate the alteration of the record, but doesn't initiate the validation of the public key certificates' status immediately.

This can result in a forgery being accepted if the key has been compromised. Furthermore, also the signer's public key credential has been authenticated, but the signed paper itself hasn't. In our case with an e-qualification certificate, the signed form itself is also a certificate, and could have a legitimate duration (e.g. the problem we are grappling with is a (certificate) matter, hence, a simple digital signature of the document alone doesn't fix the problem.

Digital Certificate Digital certificate which adopts digital signature technology, presents to the user by the authority to validate the user himself in the digital fields used to confirm a user's identity and access authorization to the network resources. Digital certificates can be extended to e-commerce operations on the internet and e-government activities, whose domain get interested in application of identity verification and data protection, like conventional financial, manufacturing, retail online purchases, public services etc.

LITERATURE SURVEY

Hao Guo [1] explains the concept of health records that are being utilized for the purpose of useful realization of various diagnosis and prognosis of disease for a particular patient. The most problematic occurrence is the lack of an effective methodology for the purpose of providing effective and tamper proof security to this data. The medical data is highly confidential data and can be a problem if it is leaked. Therefore, the authors in this publication have proposed the use of a hybrid and edge based blockchain to achieve the effective improvement in the security of the electronic health data.

Harsh Desai [2] elaborates on the blockchain platform as one of the most effective useful mechanisms that are being implemented in widespread applications across various different fields. This is due to the improved effectiveness of this platform in providing a secure and tamper-proof mechanism for the storage of different types of data. The authors in this approach have utilized the blockchain architecture for the purpose of achieving auctions that are accountable and private to improve the experience and the reliability of the entire process effectively. The approach has been useful in determining the auction winner in a secure and highly useful manner.

Emre Şafak [3] narrates that the goal of this research is to overcome the most significant challenges in the usage of Distributed ledger technology, which include administrative and operational issues. Software engineers will not interface with the Blockchain network explicitly in order to construct or operate the Blockchain network utilizing data from the Blockchain platform. Alternatively, the well-known and widely used centralized MongoDB will be employed. It will be easy to administer and enhance the Blockchain network. Furthermore, there will be a huge gain in power and productivity. This technology also provides a great deal of diversity in regards of integrating the Blockchain network within multiple components.

Shubham Sahai [4] introduces the concept of Databases and the attacks that are encountered by these database management systems. The databases are under constant attacks that are targeted to destabilize an organization or to steal the data. This is a highly problematic occurrence that is one of the most common problems faced by organizations and other critical infrastructure. This has been the mainstay of major hackers and other intruders to target the database that can lead to loss of a lot of data. This data can be sensitive data of the customers that can be targeted to achieve intrusion and other attacks that can be debilitating. Therefore, to reduce these occurrences, the authors have proposed verity, a blockchain based framework for the identification of the insider attacks on the Database management systems.

SCOPE OF THE PROJECT

Scope of Criminal Detection is explained below

Facial recognition software (FRS) is defined as a biometric tool used to match faces in images, usually from photos and video stills, against an existing database of identities. It can be broken down into three parts — detection (finding a face in an image), analysis (face mapping), and recognition (confirming identity).

An example of facial recognition technology is the auto photo tagging feature on Facebook or even Google Photos. Social media and tech giants like these map a user to the face in the photo by sorting through their existing database of uploaded images. Since facial features are much more complex than other existing

biometric methods like fingerprints and the eye's iris, FRS tools require complex, artificially intelligent algorithms.

According to a 2021 report Opens a new window by NIST, facial recognition algorithms now have an average error rate of just 0.08%, compared to the 4.1% in 2014. Neural networks and deep learning technology have significantly evolved since then, enabling significant development in 3D recognition software. It's not just the underlying algorithms, we now have more powerful microcontrollers and processors and advanced camera technology for lenses and on-chip processing. Access to this hardware in the form of smartphones has become a boon to the FRS industry.

Early this year, Juniper Research reported opens a new window that facial recognition hardware such as Apple's Face ID is the fastest growing form of biometric smartphone hardware. It is estimated that over 800 million smartphones will be using them by 2024. Considering the advancements in technology and the accelerated market growth, this would be the right time to incorporate facial recognition technology into your business.

METHODOLOGY

The methodology for Criminal Detection is developed under waterfall model architecture as shown in the below figure 1.

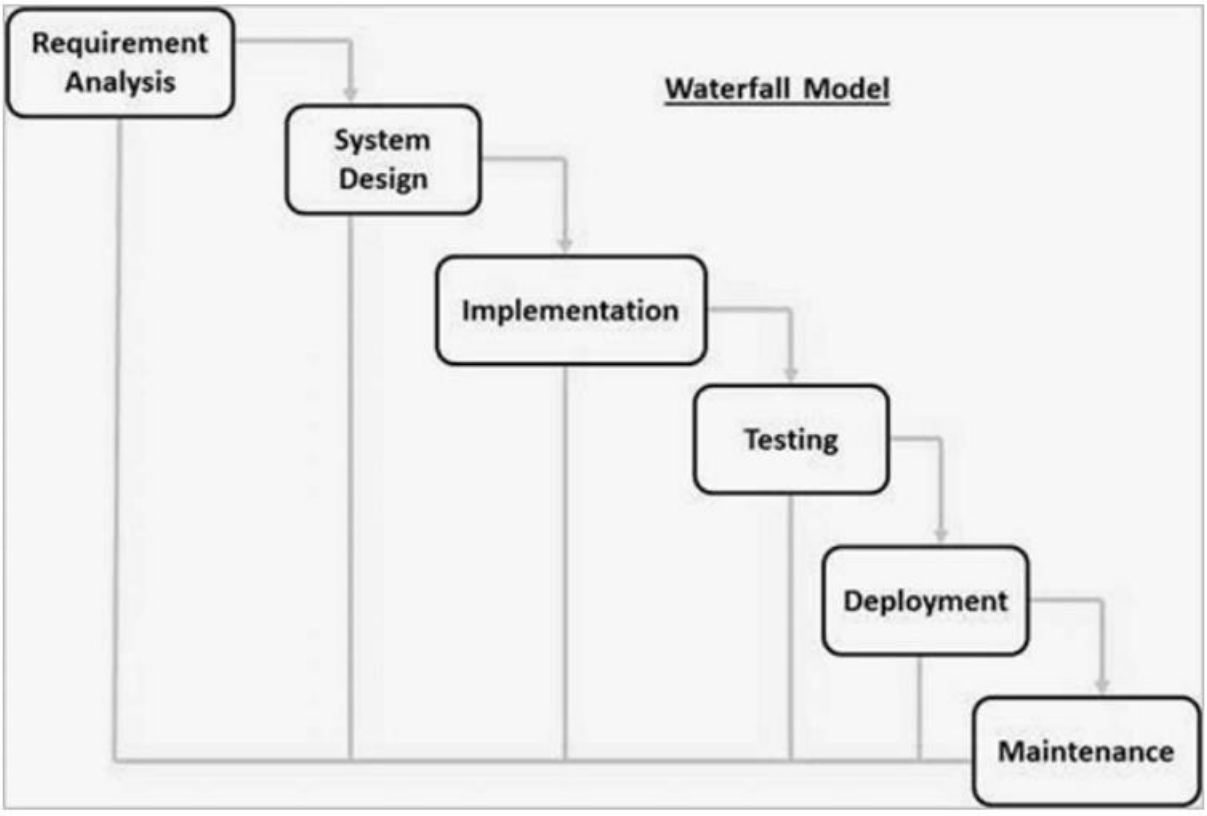


Fig 1 : Water fall model Architecture

The sequence phases in water fall model according to our project are mentioned below.

1 Requirement Analysis – Here requirement analysis are done based on following points

- ✓ Base paper for Criminal Detection System
- ✓ Studying on Convolution Neural Networks

2 System Design: The System of Criminal Detection is designed by using the following hardware and software's

1 Minimum Hardware Specification:

- Processor: Dual Core of 2.2 GHZ
- Hard Disc: 100 GB
- RAM : 2GB

2 Software Specification:

- Platform: Python , Java
- Technology : Python 3.9, JDK 1.8
- IDE: Spyder 5.0 , Netbeans 8.2
- Database : Mysql 5.0
- Libraries : Keras, Tensorflow

3 Implementation:

Proposed system is designed by using the following modules

Module A: Preprocessing

- Image Scaling
- Image Sharing
- Image restoration
- Dataset list formation

Module B: Image Normalization

- Pixel Position
- Color Model
- Model Features
- Region Estimation

Module C: Convolutional Neural Network

- ROI Extraction
- First Layer Convolution
- Fully Connected layer
- Convolution Rate

Module D: Decision Tree

- Test Image data
- Model initialization
- If-then rules
- Criminal Identification

5 Deployment of the system:

The developed software is deployed in the laptop of above mentioned configuration with the help of the mentioned software.

6 Maintenance of the system:

As this software is tested for the quick recovery, so maintenance of the system is not a challenging task. This is because the tools and the software used are open source, so there is no question of licensing the required software.

DETAILS OF DESIGN, WORKING AND PROCESSES

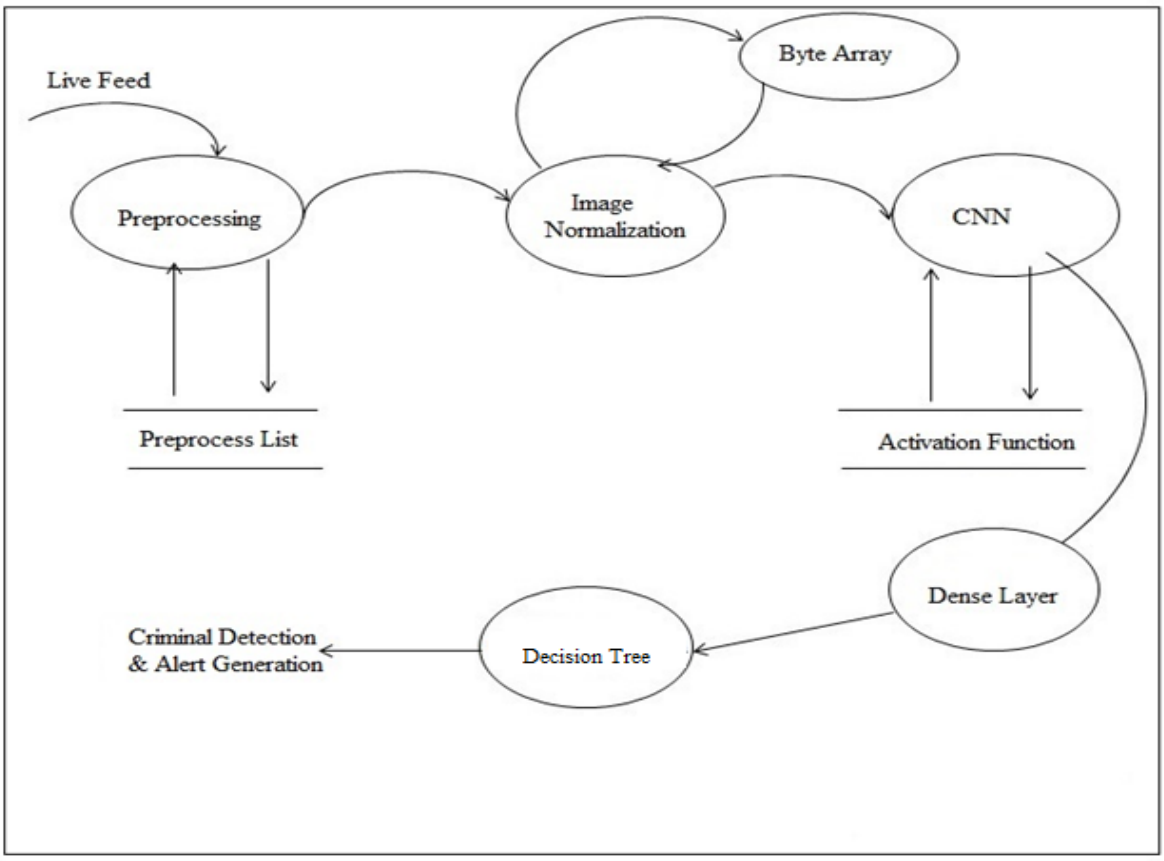
1 DETAILS OF DESIGN

1 Data Flow Diagram

DFD level 2

Fig 4 DFD level 2

The DFD 2 diagram is the most detailed wherein the user provides the Live feed from which the preprocess list is



generated and image normalization is utilized through byte array. The system then deploys CNN through Activation function and dense layer formation following which the Decision Tree is applied to get Criminal Detection and Alert generation.

3.3.2Activity Diagram

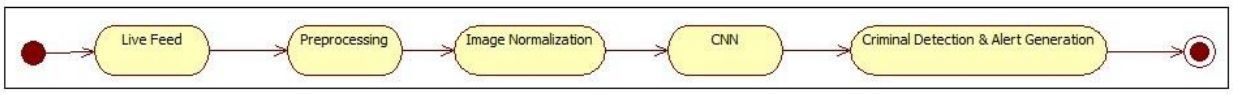
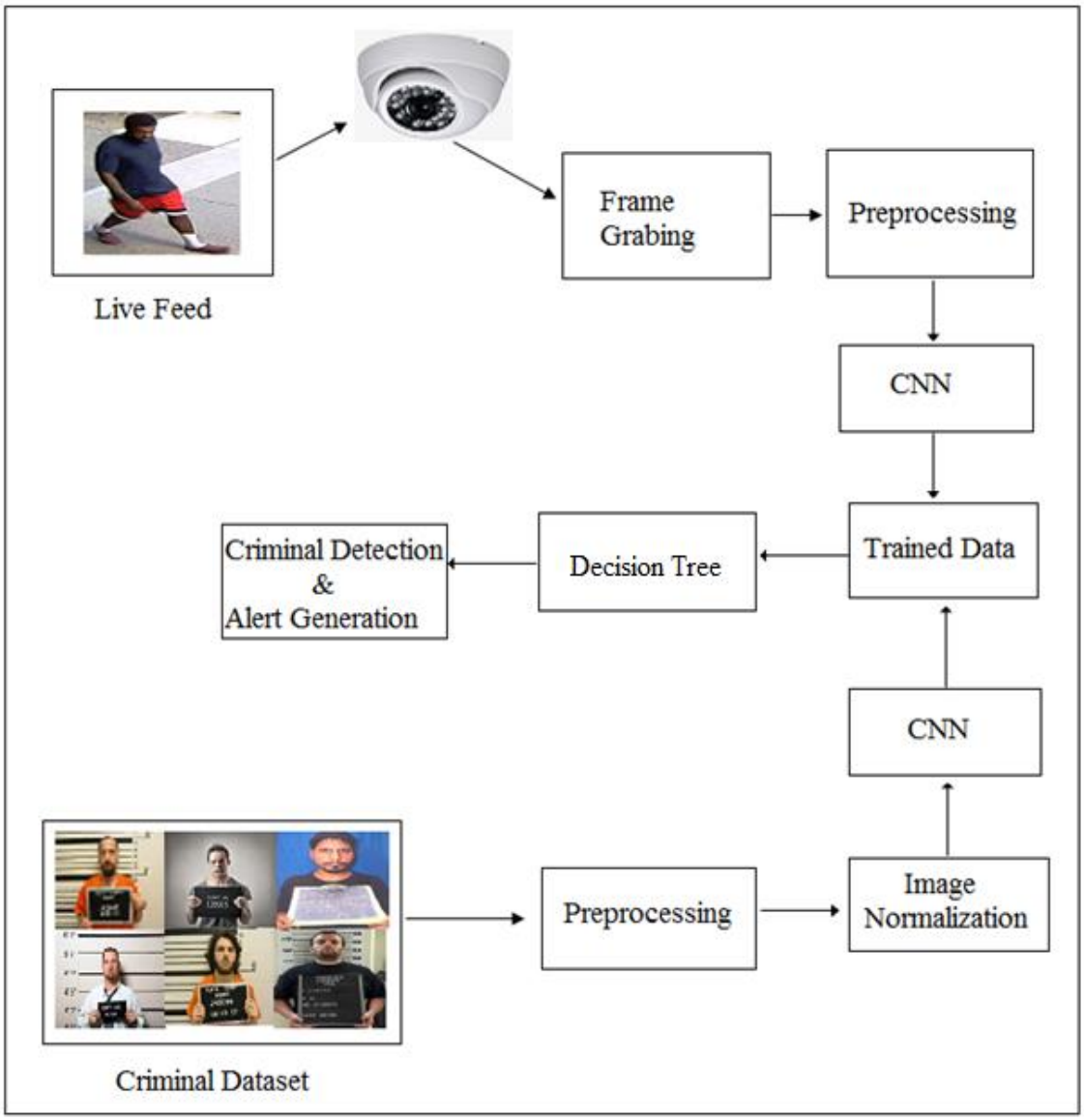


Fig 5 Activity Diagram

The activity diagram lists the various activities that are performed in the proposed methodology, the start state is initiated and the user provides the live feed, preprocessing, image normalization, CNN which results in the Criminal Detection and Alert generation.

WORKING AND PROCESSES



The system overview diagram provides an overview of the system with the important modules in the form of blocks. At first the user provides the criminal dataset which is preprocessed and the images are normalized before sending to the Convolutional Neural Networks to achieve the trained data. The user then provides the live feed the frames from which are grabbed and preprocessed following that the CNN trained data is deployed.

CONCLUSION AND FUTURE SCOPE

Criminals are the integral identity of the any society, so to unleash them a strong mechanism is required by the many sectors like banking, Woman Safety, Social Justice and other sector. The deep learning models are considered as the one of the best solution for this, Hence, this research is concentrated on the implementation of convolution neural network for the verification of the real time Criminals. This research weaved in the sense of

verifying the Criminals of the society by the law enforcement agencies. Before this process Criminal images are trained using the Convolution neural network. While testing the Criminal images are uploaded by the admin to verify it as criminal or non-criminal. If the Criminals are found then a precautionary Email will be send to Concern department through Gmail host.

FUTURE SCOPE

For the future research purpose this model can be enhanced to work as the readymade API and also as the web services to provide services to different sectors of law enforcement departments.

REFERNCES AND BIBLIOGRAPHY

[1] Dobrea, D. M., Maxim, D., & Ceparu, S. (2013, July). A face recognition system based on a Kinect sensor and Windows Azure cloud technology. In International Symposium on Signals, Circuits and Systems ISSCS2013 (pp. 1-4). IEEE.

[2] Abin, A. A., Fotouhi, M., & Kasaei, S. (2009, October). Realtime multiple face detection and tracking. In 2009 14th International CSI Computer Conference (pp. 379-384). IEEE.

[3] Tathe, S. V., Narote, A. S., & Narote, S. P. (2016, December). Face detection and recognition in videos. In 2016 IEEE Annual India Conference (INDICON) (pp. 1-6). IEEE.

[4] Lorencik, D., Ondo, J., Sincak, P., & Wagatsuma, H. (2015). Cloud-Based Image Recognition for Robots. In Robot Intelligence Technology and Applications 3 (pp. 785-796). Springer, Cham.

[5] Lin, K., Chen, S. C., Chen, C. S., Lin, D. T., & Hung, Y. P. (2015). Abandoned object detection via temporal consistency modeling and back-tracing verification for visual surveillance. IEEE Transactions on Information Forensics and Security, 10(7), 1359-1370.

[6] Chatrath, J., Gupta, P., Ahuja, P., Goel, A., & Arora, S. M. (2014, February). Real time human face detection and tracking. In 2014 international conference on signal processing and integrated networks (SPIN) (pp. 705-710).IEEE.

[7] Wu, L., Wu, P., & Meng, F. (2010, August). A fast face detection for video sequences. In 2010 Second International Conference on Intelligent Human-Machine Systems and Cybernetics (Vol. 1, pp. 117-120). IEEE.

[8] Best-Rowden, L., & Jain, A. K. (2018). Longitudinal study of automatic face recognition. IEEE transactions on pattern analysis and machine intelligence, 40(1), 148-162.

[9] Chavan, V. D., & Bharate, A. A. (2016). A review paper on face detection and recognition in video. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, 4, 97-100.

[10] Chowdhury, A. R., Lin, T. Y., Maji, S., & Learned-Miller, E.(2016, March). One-to-many face recognition with bilinear cnns. In 2016 IEEE Winter Conference on Applications of Computer Vision (WACV) (pp. 1-9). IEEE.

[11] Wang, Y., Bao, T., Ding, C., & Zhu, M. (2017, June). Face recognition in real-world surveillance videos with deep learning method. In 2017 2nd International Conference on Image, Vision and Computing (ICIVC) (pp. 239-243). IEEE.

[12] Mishra, P. K., & Saroha, G. P. (2016,

March). A study on video surveillance system for object detection and tracking. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 221-226).IEEE.

[13] Goyal, K., Agarwal, K., & Kumar, R. (2017, April). Face detection and tracking: Using OpenCV. In 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA) (Vol. 1, pp. 474-478). IEEE.

[14] Rahtu, E., Kannala, J., Salo, M., & Heikkilä, J. (2010, September). Segmenting salient objects from images and videos. In European conference on computer vision (pp. 366-379). Springer, Berlin, Heidelberg.

[15] Klare, B. F., Klein, B., Taborsky, E., Blanton, A., Cheney, J., Allen, K., ... & Jain, A. K. (2015). Pushing the frontiers of unconstrained face detection and recognition: Iarpa janus benchmark a. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1931-1939).

[16] Heshmat, M., Abd-Elhafiez, W. M., Girgis, M., & Elaw, S.(2016, December). Face identification system in video. In 2016 11th International Conference on Computer Engineering & Systems (ICCES) (pp. 147-154). IEEE.

[17] Yadhul, K., Lakshmi, P. S., & Saju, A. (2014, February). Face detection and recognition with video database. In 2014 International Conference on Electronics and Communication Systems (ICECS) (pp. 15). IEEE.

[18] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015, September). Deep face recognition. In bmvc (Vol. 1, No. 3, p.6).

[19] Singh, P., Deepak, B. B. V. L., Sethi, T., & Murthy, M. D. P. (2015, April). Real-time object detection and tracking using color feature and motion. In 2015 International Conference on Communications and Signal Processing (ICCSP) (pp.1236-1241). IEEE.

[20] Tian, Y., Feris, R. S., Liu, H., Hampapur, A., & Sun, M. T.(2011). Robust detection of abandoned and removed objects in complex surveillance videos. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 41(5), 565-576.

[21] https://azure.microsoft.com/en-in/services/cognitiveservices/face/

[22] https://biometrics.cse.msu.edu

[23] https://www.cv-foundation.org

[24] https://citeseerx.ist.psu.edu

[25] Deng, W., Chen, B., Fang, Y., & Hu, J. (2017). Deep correlation feature learning for face verification in the wild. IEEE Signal Processing Letters, 24(12), 1877-1881.