INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of First International Conference on Information Technology, Computing & Applications (ICITCA 2021)

Converging Blockchain and AI technology based Automated and Decentralized (A&D) Trust Management System using Face Detection

Pujah Balasubramaniam[1], Gokilavani Sagadevan[2]
[1,2] Meenakshi Sundararajan Engineering College, Chennai, Tamil Nadu, India.
pujahbalasubramaniam.55@gmail.com[1], ggoki5553@gmail.com[2]

Abstract

Face detection systems are growing exponentially. Newly emerged technologies are also being involved in the management applications. But they had failed to compensate at least anyone of the essential aspects of the system such as scalability, security, personalization, etc. This paper presents a fundamental platform that provides the ways and techniques to intelligently use the integration of Artificial Intelligence and Blockchain in which AI is used to detect and recognize the face and Blockchain maintains the tamper-proof records. This convergence will provide a tamper-proof and rapidly working A&D access management system for a trust management system that can be used for attendance in an organization & for many other purposes.

Keywords: Blockchain Technology, Artificial Intelligence, Decentralization, Face Detection.

1. Introduction

Face detection, as a main technology in face information science, has recently become a huge downside that is attracting more interest in the fields of pattern recognition and computer vision. It's now used in a variety of applications such as entrance protection, video secret writing, video investigation and trailing, and content-based image retrieval, among others. With the advent of engineering in recent years, the study of face detection in colour photographs has evolved into a full-fledged analysis subject. When compared to greyscale images, colour images sequences provide more information. However, it should be more resistant to various lighting conditions, advanced backgrounds, face occlusion, and expression changes, among other things. Face recognition in colour images is still a challenging process. Face detection, face recognition, and face trailing are three types of face processing. Face recognition and face trailing are used in a variety of applications, such as bad individual detection, surveillance systems, and dominant systems. Always note that the accuracy of such processes is directly proportional to the accuracy of face detection. Face recognition algorithms come in a variety of forms, each with its own set of strengths and weaknesses.[1-4]. Until recently, several analyzers were involved in face detection research, which is important in applications such as face recognition, video investigation, human-computer interface, and face image management. However, due to the nature of the target, such as voice, lighting, age, pose, the norm of the photographs and glass, hairstyle, beard, and moustaches, which may or may not be gift, and so on, many researchers have been unable to fully resolve these issues, despite having studied them for a long time. We have a propensity to include a comprehensive overview of previous work based on what we have learned from domestic and foreign discourse and research papers about face detection and facial feature position in recent years. And that, based on the previous face detection study, we established an automated face detection method.[5-8].

2. Literature Survey

They presented a fast wavelet transform based face detection algorithm in Fast Face Detection based on Wavelet Transform in the Color Image. The proposed classification algorithm was evaluated using the Caltech Web faces database and found to perform well. However, this can allow us to test the face detection algorithm on real people and map it to a hardware platform for future work. In reviewing the most recent ICCV'03 proceedings, we discovered that Xiao et al "boosting chain," though originating from an analogous principle of inheriting previous training outcomes, resulted in several strategies, of which theirs may be a full chain structure for the Discrete Adaboost system and ours may be a nested structure for the Real Adaboost framework. They presented a new TU-based face representation, LGQP, and suggested a novel PPM approach to calculate TU similarity in their paper MATCHING TEXTURE UNITS FOR FACE RECOGNITION. Integral histograms can be used to quickly calculate the PPM similarity scale. Experiments on the CMU-PIE and FERET databases revealed that our approach improves recognition accuracy significantly. However, it will use feature selection techniques to reduce the length of features created by LGQP.[9-11].

They have obtained a series of results in Explainable Deep-Fake Detection Using Visual Interpretability Methods that suggest explanations to our classifier model's predictions in terms of heatmaps or image definition slices, as well as input perturbation results that point to our model achieving rotational invariance to an outsized degree.As a result, they've demonstrated the effectiveness of our model in detecting DeepFake images from video in a way that even a layperson can understand. In terms of the regions of interest highlighted by these models, there are striking similarities, with many of them focusing their attention on similar regions in the picture.However, using XAI techniques in this way advances our understanding of complex models and offers a venue for presenting some much-needed meaning to the apparently obtuse decisions that AI cannot understand. We hope that as a result of this study, the top goal of fostering trust between AI practitioners and, as a result, target customers will be impossible to achieve.[12-15].

3. Proposed System

Fig.1: Importance of convergence

AI technologies can recognize obstacles, multiple objects and hazards from a safe distance and alert the driver. AI technologies are built into Advanced Driver Assistance Systems (ADAS) applications that work on camera and other sensor data to alert the administrator by sensing hazardous conditions on the road. Sensors are used to detect the malicious act and traffic around it. In case there is an tampering in the route of the path this system gets the information from the nearest signal or any nearest system that passed by that route. In this manner malicious activities and spoofing can be avoided. In case there is a speed bump or any damage the sensors also senses them. Each node working via this system will have a unique ID (confidence value) that indicates whether it is a person to be trusted or is it a malicious activity. The information regarding the confidence value of each vehicle is maintained by blockchain as it is decentralized and highly secured. When the system sensors communicate with one another, in case there is wrong information regarding an event or any other information the confidence value decreases. For every wrong or malicious information, the confidence value decreases. Higher the truth value more people trust the information for a error-free processing.

3.1.Scalable Blockchain

As we know, it is impossible to hack the blockchain until the third party has the majority of mining power. At the same time, the blockchain should be a scalable one. Converging AI in the chain will definitely do that.

3.2.Personalised Services

In this A&D system for Face detection, personal details of the nodes will not be shared among the network. But the nodes have to be provided with

personalized services in normal as well as emergency situations. For example, Even the receiver node's location data are not shared with the emergency message sender node, It has to get the alert if it has an issue specifically.

3.3.Contribution of Blockchain

Blockchain in Face Detection system can be used to verify node identity and login history, Track auto components through the supply chain, automate machine payments, establish a mobility commerce platform, facilitate car and ride sharing and support usage-based insurance and taxes. Through the use of blockchain technology, there are immutable records of all the data, variables, and processes used by AIs for their decision-making processes. This makes it far easier to audit the entire process. Having such individual applications both AI and Blockchain play a major role in the flourishing IT industry. But what if both the technologies are integrated. It would definitely create a new turn in the industry.The convergence of Blockchain and AI can enhance machine learning and enable AI to create and trade financial products. Blockchain enables secure storage and sharing of data or anything of value. AI can analyse and generate insights from data to generate value. This paper majorly focuses on the access management system for Face Detection. In a more simplified form the cars communicate with one another in order to avoid bumping into each other.

3.3.1. Decentralization

Decentralization is a mechanism in which control is dispersed away from the central authority in the province. The majority of existing financial and government structures are centralised, which means that there is only one higher authority in charge, such as the central bank or state properties. This strategy has a number of significant drawbacks, namely because any central authority acts as a single point of failure in the system: any high-level inefficiency, whether intentional or not, ultimately has a negative impact on the entire system.

3.3.2. Explainable AI

Despite machine learning's widespread success in creating autonomous systems capable of perceiving, learning, and acting on their own, there is a reluctance to use it in reality. Integrating Blockchain with AI will make it more explainable and acceptable in some circumstances.

3.3.3. Device Coordination

In future, there is no point in creating a technology to connect untrusting devices or automobiles. Instead, we can create a gateway that has ample of criteria to validate the peers. Here, Blockchain algorithms and computations plays a role as decentralized checkers. Anyways blockchain comes with complications such as security, scalability and efficiency. For instance, Transactions can be reversed and brought about double- spends by way of gaining majority management of a blockchain's hash rate by malicious entities. Some famous cryptocurrencies such as ZenCash, Verge, and Ethereum Classic had been victims of 51% attacks in 2018. There was a loss of $20 million ultimate year due to this blockchain protection issue. At the same time, blockchain should be scalable to the limit block size and response time are optimized. Since getting an untimely message is pointless and can become a major problem. On the other hand, AI has its own set of trust, explainability, and privacy issues. Here's another example: For the road management system to prompt data to administrators about nodes, implementing AI without blockchain is inefficient. Since all of the data in the block-network is public, incorporating AI is a critical feature for providing units with privacy.

3.4.Design Overview

The joint proof-of-work and proof-of-stake makes the basement for the A&D system from blockchain point-of-view. Confidence value is calculated for every node to evaluate their trustworthiness. Administrator node's are considered as permanent units while they are stationary among the network nodes. Positive (+1) and negative (-1) ratings are a tool to increment and decrement the confidence value. These estimations are done at the administrator level when the vehicle ratings arrive because it is considered as a database center. Using proof- of-stake alone to appoint an administrator may cause error sometimes as it only considers the head node with lofty stakes. On the other hand, in proof-of-work capacity of the units are only considered excluding the stake value. At the same time, while sending personal content in a public network AI and ML(machine learning) algorithm provides confidentiality, integrity or availability(CIA) to assets. Machine learning algorithms could be used to train & execute the

vehicles whether to give positive or negative ratings to others.

3.5Design Procedure

3.5.1. Rating and Calculating Confidence Value

Ratings are generated from nodes to decide the final confidence value of each message. Every time Nodes around a specific path and within a threshold distance will send a message to node along the same path. But there is an issue that all the messages are on the same side. To trust the real one, their distance from the intended spot/area and their rate history are considered. For that if there is totally Dj data, they will be splitted into groups such as from D1 to Dk, from Dk+1 to Dn….Dm+1 to Dj for rapid computation as it should be done in nanoseconds with the help of higher computation service. The below formula should be imposed on each node:

cin = e-din +p

Here cin denotes the confidence value of node in subgroup 'n' , 'ei' is the distance of the node from the event and 'p' represents rating history.

Sender message format:

There are a lot of advantages of using asymmetric indicator method instead of Bayesian inference method. Latency should not be there while sending alert messages to the node nearest to the spot. On the other hand, asymmetric method needs less mental & system effort to implement. Chance of providing accurate result is higher in asymmetric method than Bayesian method. And, asymmetric indicators are intuitively reasonable. If the probability of 'f/c' exceeds the threshold, it reports +1 (positively rated) to the nodes whichever sent a true information and reports - 1(negatively rated) to the vehicles which have sent false information. These confidence value of an event and rating of each vehicle will be updated in corresponding administrator of spot.

3.5.2. Head Node Confidence Value Offset Generation

At a very simple level,

Y=M.X+C

Here 'X' represents the input and 'Y' represents the corresponding outcome of calculation. In this context, 'X' may be the attributes of the nodes, Administrators and locations such as type of node, location or distance of Administrator, safety condition of an area. The objective of the algorithm is to find out the optimum 'M' and 'C' values that can give an explanation for the past records and that may additionally be used to make accurate predictions in the future 'Y' given a beforehand unseen input 'x'. This procedure of working out the 'M' and the 'C' is known as 'training'. As the automatic message being sent by node and other nodes will send their ratings to head node. But here, these can be used to calculate the offset value at head node. Here 'C' is suggested to control the sensitivity of the minor and major groups. For example, if the admin received 7 positive ratings and 5 negative ratings of certain people. While using sensitivity controlling parameters, attackers cannot make assumptions and control the large portion of nodes. Therefore, by using ML algorithms reliability of offset calculation is very high.

3.5.3. Instant Minor Selection

Here is the biggest role for integrated AI and Blockchain technology. Minor can be one of Administrators as they are stationary among the network. Applying either proof-of-stake or proof-of-work will not always give an optimized solution and all head nodes will not be utilized efficiently. To get the best case situation implementing both is necessary. Since this unified algorithm will choose the Administrator with high stake value. At the same time, AI has the responsibility to select the minor based on the availability, distance and time limit from high stake minors selected by a unified algorithm. At last, the minor will be allowed to publish its hashed block.

Conclusion

The proof-of-work and proof-of-stack functions are used in the framework described in this paper. It is made up of four modules. To make a series of static images, first grab the frame of an image. After that, colour segmentation, geometric laws, and other pretreatments are applied to each static image. To take it one by one, use the sliding window in the resulting candidate face field. Finally, all of the intercepted face areas are fed into the classifiers' qualified face detection module. The location size of the human face is returned for the area judged to be the human face by the classification result. The proposed classification algorithm was put to the test on the MSEC Web faces database and found to work well. For our future work, we intend to implement the face detection algorithm on real mages and

map the algorithm onto a hardware platform. It may be used in a variety of other domain networks in the future, such as public check-in locations and so on.

References

[1]. Junjun Lou, Qichao Zhang, Zhuyun Qi, Kai Lei:A Blockchain-based keyManagement Schemefor Named Data Networking,2018.

[2]. Shaoyong Guo, Xing Hu, Ziqiang Zhou, Xinyan Wang, Feng Qi, LifangGao:Trustaccessauthenticationinvehicularnetworksbasedonblockchain.

[3]. Wenbin Zhang,Sheng Huang,Yuan Yuan∗, Yanyan Hu, Shaohua Huang,Shengjiao Cao, Anuj Chopra:A Privacy-Preserving Voting Protocol onBlockchain,2018.

[4]. ShitangYu,KunLuv,ZhauvShao,YingchengGuo,JunZou,BhoZang:AHigh PerformanceBlockchain Platformfor Intelligent Devices

[5]. George Sedky, Amr El Mougy: BCXP: Blockchain-Centric Network Layer forEfficientTransactionandBlockExchangeover NamedDataNetworking,2018.

[6]. Hui Yang, Lin Guan, Jingwen Nan, Xudong Zhao, Yongshen Liang, QiuyanYao,AoYu,JieZhang:IntelligentOptical NetworkwithAIandBlockchain,2019.

[7]. Dong Yan, Ke Guan, Danping He, Bo Ai, Zan Li Jun Hyeong Kim, HeesangChung, ZhanGyi Zhong:Channel Characterization for Vehicle-to- InfrastructureCommunications inMillimeter-Wave Band,2020.

[8]. Aoxue Li , Haobin Jiang , Jie Zhou, And Xinchen Zhou:Learning Human-LikeTrajectory Planning on Urban Two-Lane Curved Roads From ExperiencedDrivers,2019.

[9]. YingZhang,StudentMember,IEEE,YingjieZhang,ZhaoyangAi,Member,IEEE, Yun Feng and Zuolei Hu:A Cross Iteration Estimator with Base ctorforEstimationofElectricMiningHaul Truck'sMass andRoadGrade,2018.

[10]. YingZhang,TingyuZeng,YingjieZhang,ZhaoyangAi,YunFeng:Modeladaptive torque control and distribution with error reconstruction strategy forREIDEVs,2020.

[11]. QiWang,StudentMember,IEEE,DavidW.Matolak,SeniorMember,IEEE,and BoAi , Senior Member, IEEE:Shadowing Characterization for 5-GHz Block-to-BlockChannels,2018.

[12]. Thang N. Dinh,My T. Thai:AI and Blockchain: A Disruptive Integration,2018.

[13]. YoussefWehbe,MohamedAlZaabi,andDavorSvetinovic,SeniorMember,IEEE:Blockchain AI Framework for Healthcare Records Management:Constrained GoalModel,2018.

[14]. Vivian Brian Lobo,Ronald Melwin Laban,Jetso Anakin,Shraddha S.More:ConvergenceofBlockchainandArtificial IntelligencetoDecentralizeHealthcareSystems,978-1-7281-4889-2/20/$31.00 ©2020.

[15]. Zhe Yang, Kan Yang, Member, IEEE, Lei Lei, Member, IEEE, Kan Zheng,Senior Member, IEEE, and Victor C. M.Leung:Blockchain-based DecentralizedTrust Management inVehicular Networks,2327-4662 (c)2018.