IJARSCT

ISSN (Online) 2581-9429

Impact Factor: 6.252

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Volume 2, Issue 2, July 2022

Image based Biometric Authentication for Blockchain Integrated VANETs

Ms. K. Saranya[1], M. Navaneetha[2], P. Pozhil Mathi[3], K. Janani[4]

Assistant Professor, Department of Information Technology[1]

Students B.Tech, Department of Information Technology[2,3,4]

Dr. Mahalingam College of Engineering and Technology, Pollachi, Coimbatore, India

Abstract: *Vehicle in vehicular ad hoc (VANETs) communicates guides about their traffic status remotely for further developing traffic security and effectiveness. In any case, in the security message trade process, perniciousaggressor can deduce a client's character, occupation and other delicate data through direction following, and could send off an assault that can bring about accidents. Moreover, wellbeing message trade is generallyfounded on outdoors radio, and consequently different security assaults, for example, various security attacks, such as bogus information attack and impersonation attack, also sent off to VANETs . To determinethe previously mentioned security and protection issues, we propose secure and Lightweight Face Biometric Authentication using deep learning algorithm convolutional neural network for Blockchain Integrated VANETs called VeChain. The proposed scheme is appropriate for resolving issues connected with securityand protection since it joins the sealed VeChain based plans with the side of the road unit (RSU) based plans. In light of Public Key Cryptography, the proposed plot preloads the underlying public boundaries and keys of the framework in each RSU and the On-Border unit (OBU). Moreover, this scheme accomplishsecurity and protection necessities as well as opposes normal security assaults and adulterated message transmission assault. At last, the presentation assessment shows that the proposed scheme is more effectivecomputationally and communicational than the current plans in marking and confirming VANETs messages.*

Keywords: VANET’s, VeChain, Cryptographic Key, Road Side Unit (RSU), On-Border Unit (OBU).

I. INTRODUCTION

Street transportation is the core of monetary advancement of a country. The executives of traffic [8] administrations and their viable use straightforwardly affect fruitful advancement of business and other area in nations. Giving vehicles correspondence office gives more than adequate advantage to defeat many issueson street transportation. It very well may be utilized to priorly illuminate the driver about street condition, gridlock, mishaps occurred, weather patterns, front and side distances of different vehicles, abrupt break applied by front vehicle, or unexpected obstruction in the way. This wellbeing data is utilized for examination and further to respond according to the consequence of investigation. Alongside wellbeing andsecurity of driver, the organization works with data like guide of a city, significant areas in the city, ways from the source to the objective, and interactive media information like diversion film.

1.1 VANET

Vehicular Ad-hoc Networks are self-arranging networks [5,9] laid out among vehicles furnished with correspondence offices. For a rich arrangement of uses carrying out Intelligent Highways, similar to application connected with road security, traffic [8] checking and the executives, street debacle alleviationand so out and about side framework assumes an imperative part for any VANET [6]. Vehicles continuingout and about and Road Side Units (RSUs) along the streets are hubs in the VANET [6]. For simple and successful correspondence

1.2 VANET Messages

VANET messages are sorted into two kinds [6]: administration messages and control messages, Service situated messages are additionally ordered into security messages and non-wellbeing Control messages canbe arranged into three sorts: network[5] arrangement messages , confirmation messages and organization strategy update messages.

DOI: 10.48175/IJARSCT-5827

1.3 Face Biometrics

Face Biometrics is a process of capturing a user face either by recognizing a front face or side face of a person by extracting the facial features of the features and the vectors of the face are extracted and a histogram image is processed, the face biometric [10] template can be recognized by classifying the decrypted template of the encrypted and classifying the encrypted templates without decrypting. Face acknowledgment is an innovation fit for recognizing or confirming a subject through a picture, video or anygeneral media component of his face. Face acknowledgment in static pictures and video arrangements, caught in unconstrained recording conditions, is one of the most broadly concentrated on themes in PC vision because of its broad scope of uses in reconnaissance, policing, measurements, promoting, and somemore.

1.4 Software Description

A. WAMP Server

WampServer is a web development environment for Windows. With Apache2, PHP, and a MySQL database, you can create web apps. PhpMyAdmin, on the other hand, makes it simple to administer your database. WAMP Server is a dependable web development software tool that allows you to create web apps using MYSQL and PHP Apache2. The appliance's easy interface and extensive functionality make it a popular choice among developers all around the world. The software is available without charge and does not require a subscription.

B. Python 3.7.4

Python is a high-level and object-oriented programming language. Python is simple to code the programming while comparing to other programming languages, it focuses on code readability and shorter syntax. It is easy to and simple to implement. In python programming data types are dynamic and it is not necessary to declare data types

II. RELATED WORK

VANET security correspondence can be made by two methods [6]: Periodic Safety Message and Event Driven Message (Emergency Message), both sharing just a single control channel. The Beacon messages are statusmessages containing status data about the source vehicle like position, speed, heading … and so forth. Guides give new data about the shipper vehicle to the encompassing vehicles in the organization assisting them with knowing the situation with the ongoing organization and anticipate the development of vehicles.Signals are sent forcefully to adjoining vehicles 10 messages each second. In this manner, a solid system for character validation and message uprightness is the achievement key to affirm the security of VANETs[6]. In any case, albeit prior offered confirmation plans could address some security and protection issues in VANETs [6].

III. EXISTING SYSTEM

3.1 VANET Broadcasting Message Security

VANET communication can by done safely by two means[6], the first method is Beacon Messagewhich is periodically sent by the vehicle to the neighbouring vehicle for every 10 seconds, as theseinformation's are sent periodically to other vehicles, so that everyone can be in up to date and the vehicle shares the latest information lively and periodically, so that every other vehicles can know the current moment of all other vehicles in the network[5,9] .

3.2 Key Private Proxy Re-Encryption Scheme

In key private proxy re-encryption [3] scheme keys are kept private so that a key of a user cannot beidentified or differentiated this key provides enhanced security then the pre-existing scheme, this scheme is also known as anonymous proxy re-encryption [3].

3.3 Ciphertext-Policy Attribute based Proxy Re-encryption

This encryption [3] scheme is a combination of attribute-based encryption [3] and traditional proxyre-encryption scheme. This method is used to handle the key distribution of multiple users.

3.4 Time /Clock Based Proxy Re-encryption Scheme

In Time/clockbased re-encryption [3] cloud is allowed to independently re-encrypt the dataautomatically, encryption is done only after the command sent by the sender.

3.5 VANET Driver Authentication

VANETs (Vehicular Ad Hoc Networks) [5,6] offer numerous significant types of assistance to the clients in the ad hoc [7] climate and the individual data of the clients like their geo areas, their recordsubtleties and so forth are joined with them. In the event that any dubious movement happens in the climate, makes numerous horrendous results. Whenever a vehicle needs to pass on any message, it joins the specially appointed bunch and for the sake of security it goes through some security boundaries[7]. One of these security boundaries is confirmation of vehicle in which vehicle goes through the personality check. There are numerous client confirmation plans present in VANETs [6]some of them depend on biometric [10] like fingerprints.

To rectify these issues, this paper centres around upgrading a validation scheme in light of restrictive protection safeguarding and further developing its exhibition effectiveness. This paper audits the security weaknesses of the current plans. It additionally proposes upgrades to the character based restrictive protection saving validation plan to get and work on the effectiveness of VANETs correspondence [6].

IV. PROPOSED WORK

In this undertaking We have proposed a blockchain [4] based system named VeChain and Drivers face biometrics in VANETs [6] to forestall unlawful or fake message transmission. And furthermore safeguard the protection of vehicle and guide messages by utilizing a PKI based key pair given by the TMS Server [2] to speak with different gatherings in the VANET climate [6]. For Face Authentication ofdriver's, we utilized profound learning calculation named DCNN [1].

4.1 Face Recognition using CNN

Face acknowledgment is tracking down its direction into the new ages of vehicles trying to expand wellbeing and accommodation. From vehicle start to robbery avoidance - there are innumerable potential outcomes of involving facial acknowledgment in vehicles. Face acknowledgment deals with a straightforward and non-prominent rule. After a driver selects into the framework, the framework "recallsthat" them. Each time they enter the vehicle once more, the framework "remembers" them and gives themadmittance to predefined functionalities, for example, the authorization to begin the vehicle.

4.2 Face detection

The OBU identifies faces in a video transfer. When the face is caught, the picture is edited and shipped offthe TMS through HTTP structure information demand. The back-end API saves the picture to a nearby document framework and recoveries a record to Detection Log with a Driver ID.

4.3 Instant Face Recognition

The back end has a foundation CNN [1] calculation that observes new unclassified records and uses drivers selected library to compute the 128-layered descriptor vector of face highlights. At the point whena vector is determined, it is contrasted and different reference face pictures by ascertaining Euclidean distance to each element vector of every Person in the data set, tracking down a match.

4.4 PKI–Public Key Cryptography

Public key cryptography is a process of involving a private key and and a public key and it is used to authenticate, private key is also known as secret key Public key cryptography enables encryption and decryption feature here public key is used for encryption and private key is used for decryption and alsouses two keys that are mathematically encrypted, publick key cryptography is not like symmetric key cryptography.

DOI: 10.48175/IJARSCT-5827

4.5 VeChain Integration

In this paper, we propose the utilization of a permissioned consortium blockchain [4] framework with shrewd agreement highlight named VeChain. The utilization of a permissioned consortium blockchain [4]mitigates security gambles related with the intricacies in interorganizational information taking care of, forexample, in the space of access control, information uprightness, privacy, and accessibility. This clever VeChain configuration is reasonable for safeguarding the security of wellbeing messages inside VANET [6] in certifiable situations. The blockchain [4] will hold and oversee occasion message history close by every vehicle's trust level dependably, permanent, and with great dispersion. Each nation will have one remarkable blockchain [4] with free administration and upkeep to record vehicle data.

V. OBJECTIVES OF THE PROPOSED SYSTEM

Low calculation and correspondence upward: The correspondence among vehicles and RSU stays in one piece for a couple of moments. Subsequently, all expected correspondence and calculation cycles ought tobe performed rapidly.

- Message integrity: Every message must be conveyed with no adjustments and the message's information trustworthiness ought to be guaranteed.
- Message legitimacy: The message source ought to be validated to forestall the pantomime assault. Privacy preservation: The genuine character of vehicles ought to be safeguarded during correspondence.Be that as it may, the specialists ought to have the option to track down the genuine personality of any vehicle in remarkable cases, like risk examination.

5.1 Alorithm

- Step 1: If the user is a first-time visitor, they must register by clicking the sing in button.
- Step 2: After that, the user must fill out the registration form.
- Step 3: Now the prompts for video recording will appear, and a 10-second facial video will becollected, as well as a fingerprint image.
- Step 4: Frames will be created from video captured.
- Step 5: User ids are now transformed into hash values and photos are converted into encryptedtemplates using logistic map.
- Step 6: The discrete wavelet transform is used to classify fingerprint images.
- Step 7: After encryption, the hashed user id and face template are saved.
- Step 8: If the user already has an account, he must supply his user id.
- Step 9: The crypto server retrieves the hashed user id and encrypted templates for the matching user.
- Step 10: In the crypto server, the encrypted templates are now decoded.
- Step 11: Deep convolution neural networks are used for classification.
- Step 12: If the decrypted templates match the user's current face and finger print image, the user isgranted access to the untrusted server.

5.2 System Flow

The user enrols the vehicle number with his corresponding face biometrics. Now the its all set to login.Whenever the event detected like accident immediately encrypted message is sent to road side unit (as shown in figure 1.1), then the Road Side Unit verifies the message before transmitting it to the TrustedAuthority. Now the message is broadcasted to the block chain network so that every car in the smart contract can receive the encrypted message through road side unit and further message can be downloaded and decrypted by the nearby vehicle

DOI: 10.48175/IJARSCT-5827

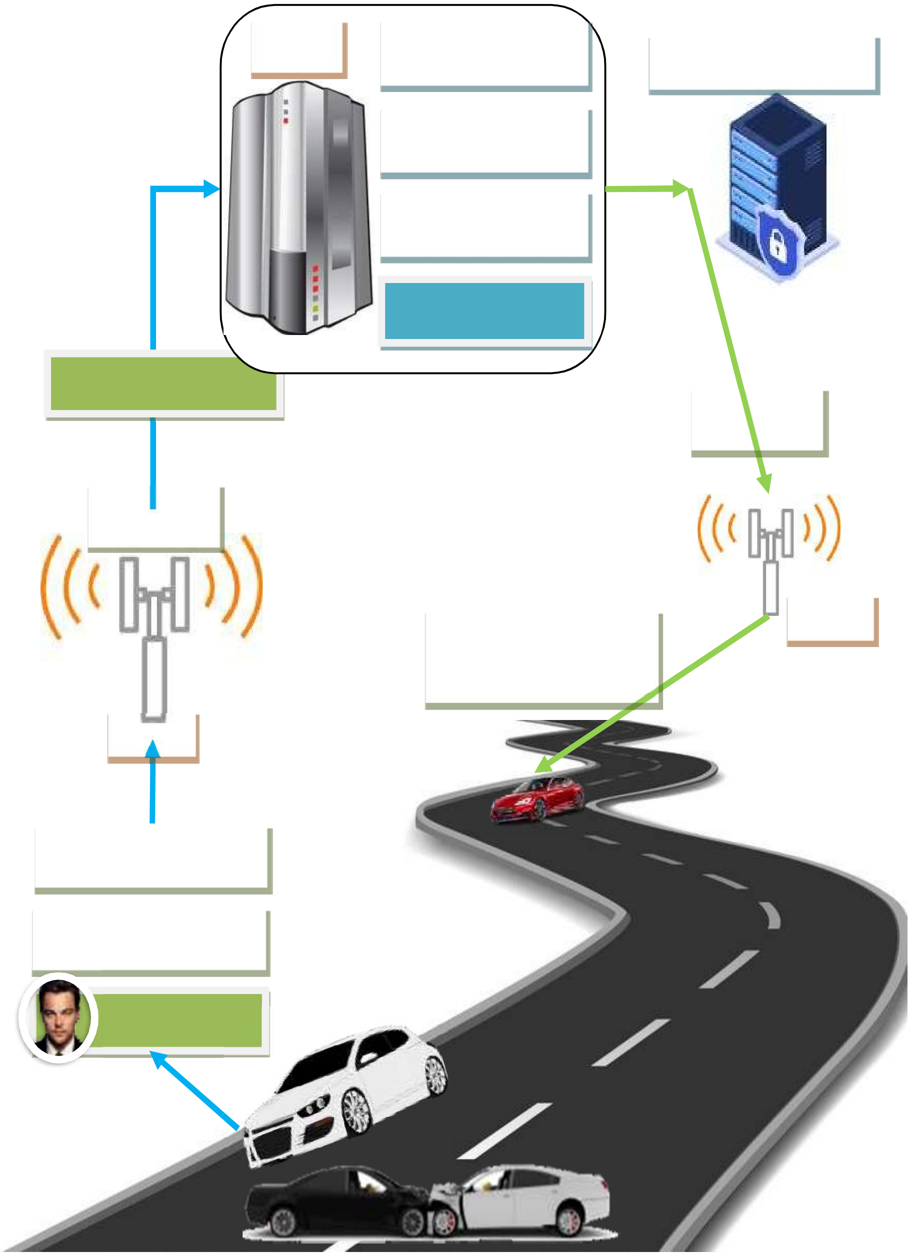


Figure 1.1: System Architecture

VI. MODULE DESCRIPTION:

6.1 Traffic Management Server

The traffic the executives server [2,8] is liable for instating the framework, conveying shrewd agreements,enlisting vehicles and repudiating enrollments. TMS to give the endorsements and public keys to the vehicles after the confirmation cycle is finished from Motor Vehicle Department[8].

6.2 Vehicle Registration Phase

The vehicle clients are expected to present their unique accreditations, for example, address and mail-id to the during the hour of enrollment to enter inside the VANET [6] framework.

6.3 PKI Key Generator

Public/Private Key Generation: RSA Asymmetric calculation is utilized to create the key matches. It is executed by KGC in TMS taking the vehicle public boundaries params and the incomplete private key dias information. KGC yields vehicle public key PKi and private key SKi.

6.4 Vehicle Face Biometric Authentication

A. Face Registration

During the enrollment stage when vehicle data alongside driver's detail will be shipped off TMS[10]. Thisdata will contain the essence of the driver to guarantee the character. The on-board unit (OBU) will camera.The validation of the driver's personality will be finished utilizing Deep Convolutional Neural Network (DCNN) [1,9]. Face Image pre-handling are the means taken to arrange pictures before they are utilized bymodel preparation and deduction(as shown is Figure:1.2)

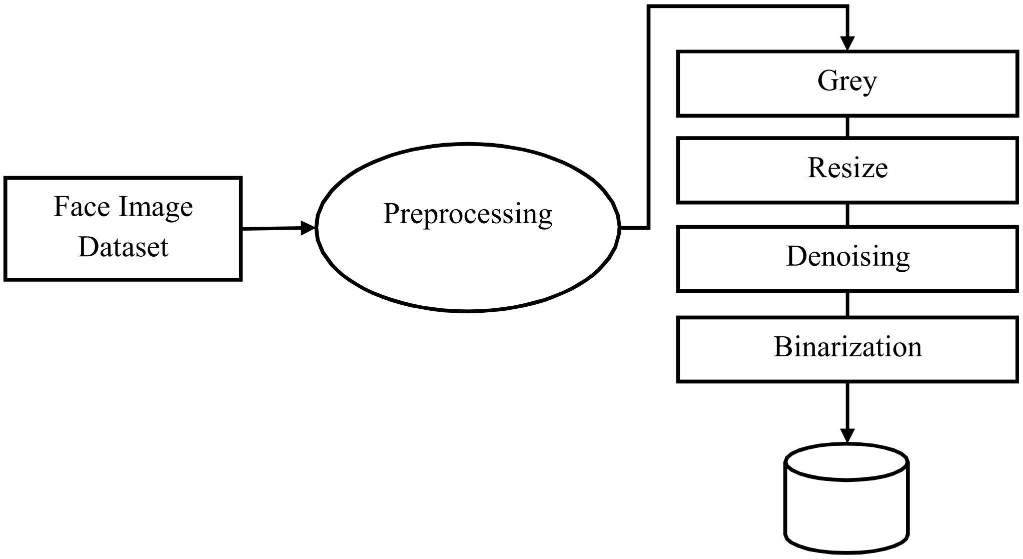


Figure 1.2: Face Pre-processing

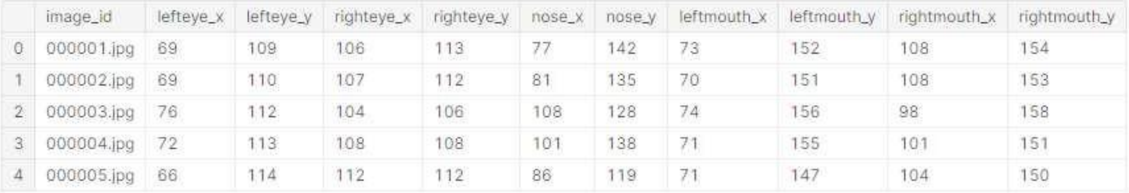
B. Gray Level Co-occurrence Matrix

GLCM is a second-request factual surface investigation strategy. It analyzes the spatial relationship amongpixels and characterizes how regularly a mix of pixels are available in a picture in a provided guidance Θ and distance d. Each picture is quantized into 16 dark levels (0-15) and 4 GLCMs (M) each for Θ = 0, 45, 90, and 135 degrees with d = 1 are gotten. From each GLCM, five highlights (Eq. 13.30-13.34) are separated. Subsequently, there are 20 highlights for each picture. Each element is standardized to go between 0 to 1 preceding passing to the classifiers, and every classifier gets similar arrangement of highlights.

The highlights we separated can be gathered into three classes. The principal classification is the main request measurements, which incorporates most extreme power, least force, mean, middle, tenth percentile, 90th percentile, standard deviation, difference of force esteem, energy, entropy, and others.

Sl. No	GLCM Feature	Formula
1.	*Contrast*	$\sum_{i,j=0}^{N-1} P_{i,j}(i-j)^2$
2.	*Correlation*	$\sum_{i,j=0}^{N-1} P_{i,j}\left[\frac{(i-\mu_i)(j-\mu_j)}{\sqrt{(\sigma_i^2)(\sigma_j^2)}}\right]$

3.	*Dissimilarity*	$\sum^{N-1} P_{i,j}\,\lvert i - j\rvert i, j = 0$
4.	*Energy*	$\sum_{i,j=0}^{N-1} P^{2}_{i,j}$
5.	*Entropy*	$\sum_{j=0}^{N-1} P_{i,j}\,(-\ln P_{i,j})i,$
6.	*Homogeneity*	$\sum_{i,j=0}^{N-1} \frac{P_{i,j}}{1+(i-j)^2}$
7.	*Mean*	$\mu_i = \sum_{j=0}^{N-1} i\,(P_{i,j})\,, \quad \mu_j = \sum_{i,j=0}^{N-1} j\,(P_{i,j})i,$
8.	*Variance*	$\sigma^2_i = \sum_{i,j=0}^{N-1} P_{i,j}\,(i-\mu_i)^2\,, \quad \sigma^2_j = \sum_{i,j=0}^{N-1} P_{i,j}\,(j-\mu_j)^2$
9.	*Standard Deviation*	$\sigma_i = \sqrt{\sigma^2_i}\,, \quad \sigma_j = \sqrt{\sigma^2_j}$



	image_id	lefteye_x	lefteye_y	righteye_x	righteye_y	nose_x	nose_y	leftmouth_x	leftmouth_y	rightmouth_x	rightmouth_y
0	000001.jpg	69	109	106	113	77	142	73	152	108	154
1	000002.jpg	69	110	107	112	81	135	70	151	108	153
2	000003.jpg	76	112	104	106	108	128	74	156	98	158
3	000004.jpg	72	113	108	108	101	138	71	155	101	151
4	000005.jpg	66	114	112	112	86	119	71	147	104	150

C. Face Classification

DCNN[1] calculations were made to naturally identify and dismiss inappropriate face pictures during the enrolment interaction. This will guarantee appropriate enrolmentand subsequently the most ideal execution.

D. Face Identification

Subsequent to catching the face picture from the Vehicle OBU Camera, the picture is given to confront discovery module. This module identifies the picture districts which are probably going to be human. As shown below in Figure 1.3.,

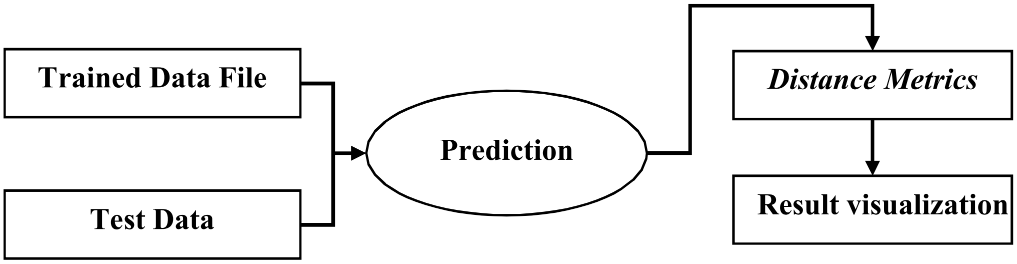


Figure 1.3. Face Identification flow

6.4 Performance Analysis

A. Face Recognition Performance Analysis

The significant focuses engaged with the exhibition measurements are examined in light of the setting ofthis task:
Genuine Positive (TP): There is a Face, and the calculations distinguish Vehicle Driver.
Bogus Positive (FP): There is no Face, however the calculations identify as Driver and show Driver name.False Negative (FN): There is a Face, however the calculations don't identify Driver and name.
True Negative (TN): Face is not identified, and there is nothing disthinguished

B. Accuracy

Accuracy is a an process of analyzing the performance of the algorithm and testing the performance of thealgorithm accuracy is how best is performing. Accuracy is calculated using the following formula .
Accuracy = (T P + T N)/ (T P + T N + F P + F N)Accuracy: 0.9984025559105432

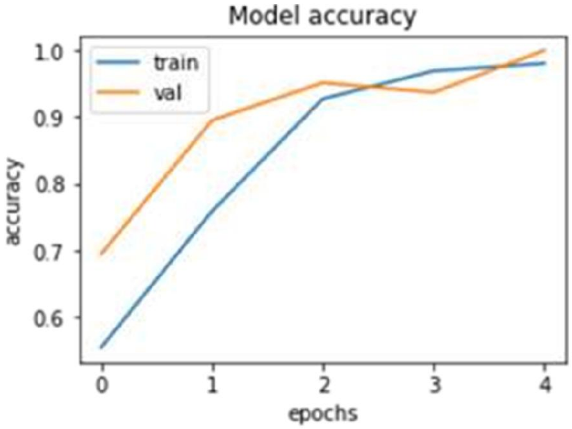


Figure 1.4. Accuracy

C. Precision

It signifies the proportion of decidedly anticipated cases that are really sure. With regards to this theory, accuracy estimates the negligible part of items that are anticipated to be Card Holder and are really Card Holder Face present in ATM climate. Accuracy is determined utilizing the accompanying equation.
Accuracy = T P/(T P + F P)Accuracy: 0.9990234375

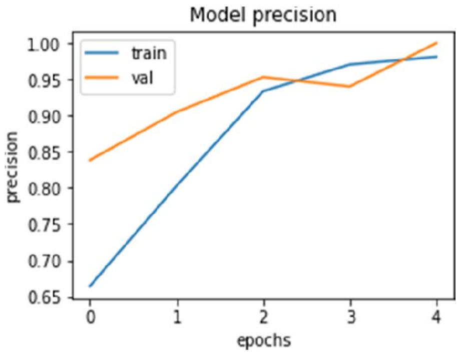


Figure 1.5. Precision

D. Recall

It signifies the proportion of decidedly anticipated cases that are really sure. With regards to this theory, accuracy estimates the negligible part of items that are anticipated to be Card Holder and are really Card Holder Face present in ATM climate. Accuracy is determined utilizing the accompanying equation.
Accuracy = T P/(T P + F P)Accuracy: 0.9990234375

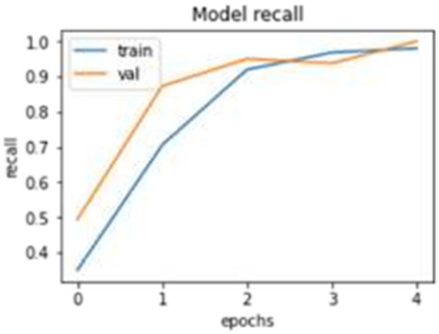


Figure 1.6. Model Recall

E. F1 Score

It is otherwise called adjusted F-score or F-measure. F1 score is a proportion of exactness of a model joining accuracy and review. With regards to this postulation, a decent F1 score shows that there are lessmisleading up-sides and bogus negatives. This shows that the model is accurately recognizing Face in ATM climate. A model/calculation is viewed as great assuming F1 score is 1. It is determined utilizing the accompanying equation.
F1 = 2 × (Precision × Recall/Precision + Recall)F1_score: 0.9977122020583142.

VII. CONCLUSION

VANETs [6] establishes an open access climate that presents critical difficulties as far as security and protection, delivering it unsatisfactory for certifiable execution. The protection and verification of the information and vehiclist were the greatest worries of specialists in VANET [6] to work on the security. Spurred by this, a blockchain-based [4] unknown confirmation plot is proposed in this paper for giving secure correspondence in VANETs[6]. In this undertaking a biometrics blockchain [4] (VeChain) systemis proposed to make correspondence in VANET safer[6]. The biometrics highlights are joined with blockchain [4] innovation to give solid transmission of information, following the information traded andID of the vehicle capable on account of erroneously messages. In the proposed plot, the RSUs can really validate the vehicles in an unknown way, and they additionally perform future interchanges through the common meeting key. Also, the trustworthiness of the sending message is totally safeguarded to keep away from distorted information transmission assault because of the help of the blockchain [4]. The presentation investigation segment demonstrated that the VeChain is proficient as far as computational expense, stockpiling cost, and correspondence cost, thus, it is profoundly viable for continuous applications

VIII. FUTURE ENHANCEMENT

In ongoing works, it is chosen to foster VeChain-helped proprietorship trade conventions which permit thehandover of responsibility for vehicle client to one more vehicle client in a solid and conveyed way duringthe hour of vehicle exchanging and furthermore purchase another vehicle

REFERENCES

[1]. Jing Lia,b, Xiaohui Kuangc,∗, Shujie Lina, Xu Mad, Yi Tange 2020, Privacy preservation for machinelearning training and classification based on homomorphic encryption schemes.

[2]. Vinod Ramesh Falmari, M. Brindha ∗-2021-,Privacy preserving biometric authentication usingChaos on remote untrusted server.

[3]. M. Gayathria,∗, C. Malathyb -2021, Novel framework for multimodal biometric image authenticationusing visual share neural network .

[4]. Dhanesh Kumar, Anand B. Joshi ∗, Sonali Singh-2021,A novel encryption scheme for securingbiometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system.

[5]. M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, "LSWBVM: A lightweight security without utilizing cluster confirmation strategy conspire for a vehicle specially appointed network,"

DOI: 10.48175/IJARSCT-5827

IEEE Access, vol. 8, pp. 170507-170518, 2020.

[6]. Sheikh, Liang, and Wang, "A review of safety administrations, assaults, and applications for vehicular adhoc organizations (VANETs)," Sensors, vol. 19, no. 16, p. 3589, Aug. 2019.

[7]. X.Yang, X.Yi, I. Khalil,Y. Zeng, X. Huang, S. Nepal, X.Yang, and H. Cui, "A lightweight verification plot for vehicular ad hoc organizations in view of MSR," Veh. Commun., vol. 15, pp. 16-27, Jan. 2019.

[8]. Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing clog assault on arising associated vehicle-based traffic light control," in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), 2018, pp. 1-15.

[9]. M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of validation and security plans in vehicular specially appointed networks," IEEE Sensors J., vol. 21, no. 2, pp. 2422-2433, Jan. 2021.

[10]. V. Talreja, M.C. Valenti, N.M. Nasrabadi, Deep hashing for secure multimodal biometrics, IEEETrans. Inf. Forensics Secur. 16 (2020) 1306–1321.

[11]. J. Cui, J. Zhang, H. Zhong, and Y. Xu, ``SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," IEEE Trans. Veh. Technol., vol. 66, no. 11, pp. 10283-10295, Nov.2017.

[12]. M. Azees, P. Vijayakumar, and L. J. Deboarh, ``EAAP: Efficient anonymous authentication withconditional privacy-preserving scheme for vehicular ad hoc networks," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 9, pp. 2467-2476, Sep. 2017.

[13]. Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, ``Vulnerability of traffic controlsystem under cyberattacks with falsihed data," Transp. Res. Rec., J. Transp. Res. Board, vol. 2672, no. 1, pp. 1-11, Dec. 2018.

Authors' Background

Name	**Research Field**	**Personal website**
M Navaneetha	Blockchain Technology	navimanickam422@gmail.com
P Pozhil Mathi	Blockchain Technology	pozhilprasad26@gmail.com
K Janani	Blockchain Technology	jananikrish06102000@gmail.com