JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

SMART HOME SECURITY FOR FACIAL RECOGNITION USING IOT

[1]R.Srinivas,Associate Professor,Department of IT,
Vignan's Nirula Institute ofTechnology and Science for Women, Peda Palakaluru, Guntur.
[2]P.V.N Vamsi Lala,Assistant Professor, Department of IT,
Vignan's Nirula Institute ofTechnology and Science for Women, Peda Palakaluru, Guntur
[3]Battini Bhavani , [4]Koppanathi Suhasini ,[5]Dulipalla Manasa ,[6]Meesala HemaLatha,
[3,4,5,6]BTECH,Department of IT, Vignan's Nirula Institute of Technology and Science for Women, Peda Palakaluru, Guntur.

Abstract:

One of the main concerns in the current society is security. One of the biggest issues facing the modern world is security. As technology develops, more security issues arise. Current security protocols contain certain flaws and are susceptible to hackers. Based on Internet of Things (IoT), the proposed solution to the security issue is based on facial detection and identification.

The camera takes a picture of a person's face, which is then compared to the acquired database. The authorized user may utilize a mobile application to provide any unregistered person access to the premises. If someone enters without permission or knowledge, a picture of their face will be taken and emailed to the appropriate authorities. An alarm will sound if someone tries to enter without authorization. The proposed system produced accurate results for both authorized and unauthorized users.The introduced system provides a low-cost solution for monitoring and controlling the houses, different organizations like banks, universities, etc. In this study, using the CNN Alexnet facial recognition system which is implemented in a door locking system, data collection is done which is then used to train machine learning where the results are quite accurate where the accuracy is the result is 97.5% which is quite good compared to some other studies. The conclusion is the CNN method can perform facial recognition which is quite accurate which can be implemented on the IoT device.

KEYWORDS:

Smart Home Security,Facial Recognition,Internet of Things (IoT),Biometric Authentication,Home Automation,Surveillance System Real-time Monitoring,Smart Cameras,Machine LearningComputer Vision.

1.Introduction:

Face recognition is important not only because it allows[1-2] us to use our face as a key but also because systems like[3-5] face identification can read our expressions in real time.[6-9] As IoT grows, different devices are being developed and face recognition is emerging rapidly. Now-a-days, security is the major

issue for every person. People get[10-15] harassed in their house and old security methods have failed to provide a high level of security.Different electronic devices, such as mobile phones, laptop and ATM, used some type of biometric[16-20] authentication or passcode but these can be easily accessed by thieves by any means which is not safe. Over the past few years, there have been quite a several choices in conventional[21-30] technology and biometric technology to meet security needs for households or offices. Some conventional security systems, for example using keys,

passcodes,[31-36] ID cards, and/or RFID cards, can be unreliable if objects for access are stolen or lost. Such security systems have disadvantages when access is stolen by people who do not have the authority to gain[37-41] access and also daily activities sometimes force someone to leave the house empty, such as during work or school hours. This makes the house vulnerable to break into and theft, even when the house is locked or securely locked. The development of Information Technology and Communication currently offers[42-47] convenience to users in various lines of life. One technology that is currently trending is the smart home or what is commonly known as the smart home. A smart home is a term used to define a residence that has the equipment, lighting, heating, air conditioning, TV, computer, audio system, video entertainment, security, and camera systems that can communicate with each [48]other and can be controlled remotely with a timetable. through the internet or telephone. Biometric systems are developing rapidly, especially for home security technology because they can fulfill two functions, namely identification, and verification, biometrics have characteristics that cannot be lost, cannot be forgotten, and cannot be faked where their inherent presence in humans will differ between humans and other humans so that their uniqueness is guaranteed.In the journal facial recognition as authentication is very good because the face is a physiological feature that is easiest to distinguish between individuals so face recognition is one of the biometrics technologies that are often studied and developed.Convolutional Neural Networks combines three basic architectures, namely local receptive fields, shared weight in the form of filters, and spatial subsampling in the form of pooling.Convolution or what is commonly known as convolution is a matrix that functions to perform filters. In the filtering process, there are two matrices, namely the input value matrix and the kernel matrix. That have been determined during the training process, namely Convolutional Layer, Pooling Layer, and Fully Connected Layer.The architecture that is owned by the Convolutional Neural Network can be seen in Fig. The previous paper described a prototype of a safe room access control system based on facial recognition. This system consists of a webcam to detect faces and a solenoid door lock to access the room. Every user detected by the webcam will be checked for compatibility with the database on the system using the Haar cascade classifier method embedded in OpenCV. If the user has access rights, the solenoid door lock will open and the user can enter the room.

2.Literature Survey:

Patel, K.K., Patel, S.M.:The term "Internet of things" describes a [50]kind of network that uses information-sensing devices in compliance with predefined standards to link anything to the Internet.

communication necessary for intelligent [51]tracking, monitoring, and management. This article provides an overview of IOT, including details on its definition, support for various technologies, architecture, features, and applications, as well as its functional perspective and future challenges.

Chin, H.:Face is the representation of one's identity. Hence, we have proposed an automated student attendance system [52]based on face recognition. Face recognition system is very useful in life applications especially in security control systems. The airport protectionsystem uses face recognition to identify suspects and FBI (Federal Bureau of Investigation) uses face recognition for criminal investigations. In our proposed approach, firstly, video framing is performed by activating the camera through a userfriendly interface.

Senthilkumar, G., Gopalakrishnan, K., Kumar, V.S.:An external processing [53]unit and interface devices are not necessary for an image capture system with integrated computing to extract information from photos and make the results available to other devices. Selecting an embedded platform is a very special and straightforward process. The study suggested an embedded system based on a Raspberry Pi board for picture capture. Embedded Image Capturing using Raspberry Pi system (EICSRS) was ultimately realized by taking into account the needs of the image capturing and recognition algorithm, Raspberry Pi processing module, and its peripherals, implementing based on this platform.

Sowmiya, U., Mansoor, J.S.:The concept of secure locking automation with IOT for door unlocking systems to give our houses, bank lockers, and associated control operations and security precaution via the GSM module the necessary security.It makes use of an embedded system based on a Raspberry Pi server system for picture capture. The Raspberry Pi (RPi) manages the video camera, capturing images and activating a relay to open doors. A secured facial recognizer for automated door unlocking is included in the module. The face image captured by the camera is compared to the image saved in the database.The door lock will unlock if the database has the picture; if not, an SMS alerting users to an attempted intrusion will be sent.

Wati, D.A., Abadianto, D.:In the modern world security is one of the major issues. As technology is getting advanced many security issues are arising. The existed developed security methods have some flaws and they can be hacked. The proposed system for resolving the security issue is based on face detection and recognition using Internet of Things (IoT). The face of a person is captured by the camera and compared with the acquired database. The authorized user can also utilize mobile application to give access to the premises to any unregistered person. In the case of unauthorized/unknown access, the face image of the person will be captured and notified to the concerned authorities through an email.

Lwin, H.H., Khaing, A.S., Tun, H.M.:Most doors are controlled by persons with the use of keys, security cards, password or pattern to open the door. Theaim of this paper is to help users for improvement of the door security of sensitive locations by using face detection and recognition. Face is a complex multidimensional structure and needs good computing techniques for detection and recognition.The door will open automatically for the known person due to the command of the microcontroller. On the other hand, alarm will ring for the unknown person.

3.Methodology:

Proposed System:

The main controller in our suggested system is a Raspberry Pi, which is reasonably priced and runs on very little power. It contains inbuilt sensors, such as ultrasonic distance sensors and PIR motion detection.

The Raspberry Pi-controlled door lock and unlock mechanism is assisted by the stepper motor. Display in the provided flowchart.

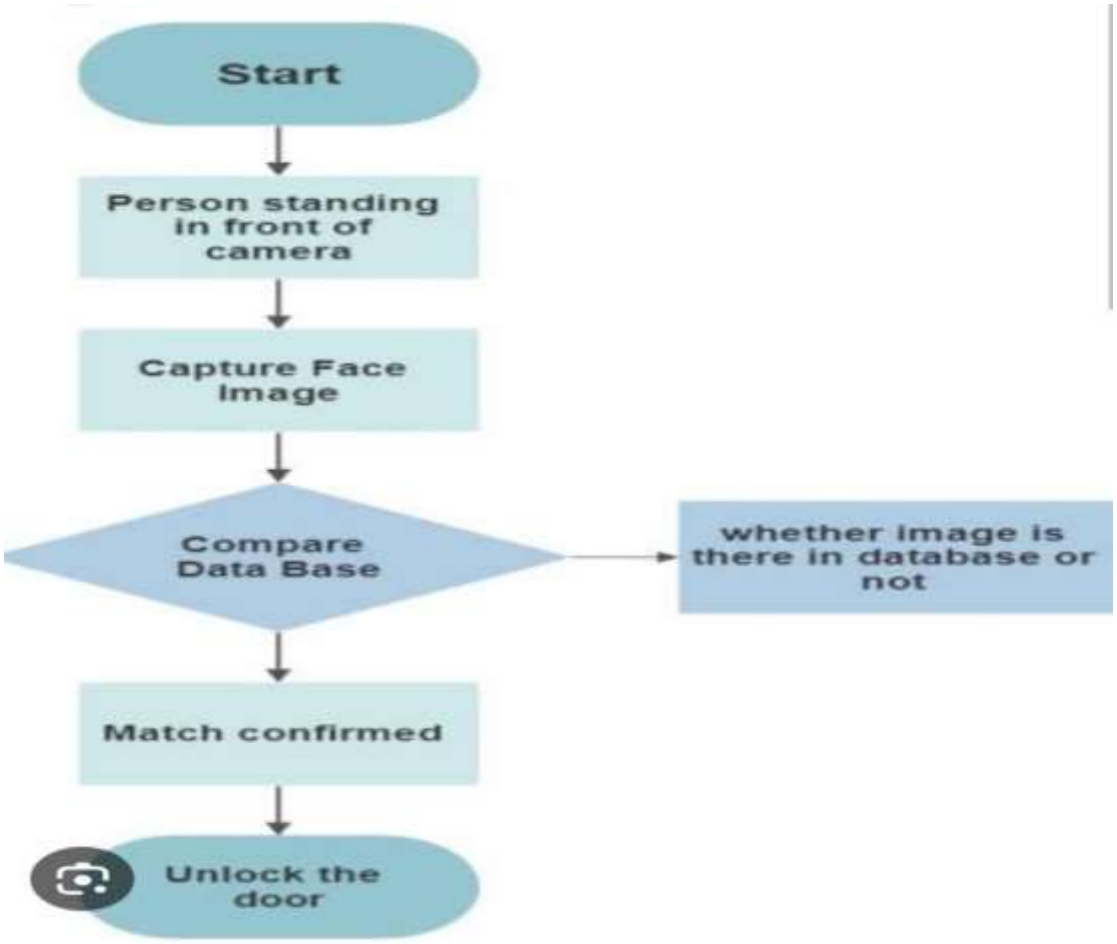

Fig1:Flow Chart

In our proposed system we have used the cloud to send the data to the remote Smartphone which is at the user side. This is the IoT basedsystem and can be made automated as and when required. It has very low power requirement which makes it most affordable. It requires minimum 5V to work. We can easily replace any part of this system without disturbing the other parts. The system will consist of the identified member's photos in the database. Any new entry can be made as andwhen required in the database. Image will be captured and face recognition will be performed. If face match found the door will open else red color bulb will light up, if the owner is at home(specified in android application) then bell will ring else notification will be sent i.e., someone is waiting outside your home.If the person is not identified, the owner will receive an email on his Gmail account with the photo of the unidentified person. All of these activities are kept in the database, which is kept on a 32GB micro SD card in a Raspberry Pi. Since all of the data is accessible online, our system operates more effectively.

Pattern in Local Binary:

Texture categorization is necessary for face identification. In this instance, the Local Binary Pattern (LBP) technique is used. The simple yet very powerful LBP texture operator thresholds the pixels around each pixel in an image to assign a binary number to that pixel. When it was first described in 1994 (LBP), it was found to be a useful feature for texture classification.

Furthermore, on some datasets, it has been demonstrated that combining LBP with the histograms of oriented gradients (HOG) descriptor significantly improves detection performance. The local representation of texture is ascertained by LBP by comparing each pixel to its near surroundings. The image must be converted to grayscale in order to be used as a texture description.

Raspberry Pi:

The Raspberry Pi is a reasonably priced Linux computer that also features a set of GPIO (general purpose input/output) pins that enable you to control electronic components for physical computing and conduct Internet of Things (IoT) experiments. It displays the Raspberry Pi GPIO.People all across the world use Raspberry Pis for hardware projects, industrial applications, home automation, and teaching programming. The suggested method uses Python programming to manage the GPIO pins. Any GPIO pin can be configured as an input or output by using the included software.

The Raspberry Pi functions inside the open source community. Raspbian is the primary supported operating system.

Fig2:Raspberry Pi

IOT Platform:

We have utilized the Ubidots framework for IoT [17]. We have employed IoT to make our houses smarter and more safe. when someone not allowed attempted to enter The owner will receive an email with the photo of the illegal individual. The owner can use the internet to monitor and operate his home's door even if he is far away. if the owner wishes to allow someone who isn't permitted to enter the house. He only needs to grant access for the door to be opened.

4.RESULTS :

After capturing the photo at the door face recognition is done to check whether person is a home member or identified one. It will determine if the person is stranger or not. If the person is stranger then door will not open. If the person is a stranger then his photo will be sent to the owners Gmail ID, the photo is shown in the given figure1 recognition is done to check whether person is a home member or identified one. It will determine if the person is stranger or not.

Fig3:unknown person identify sent to gmail

In the future a more accurate and exact face recognition algorithm can be presented. We can control the access to the door using our Smartphone remotely by sending the signals to the system. We can build an Android application to control our system more easily and efficiently.

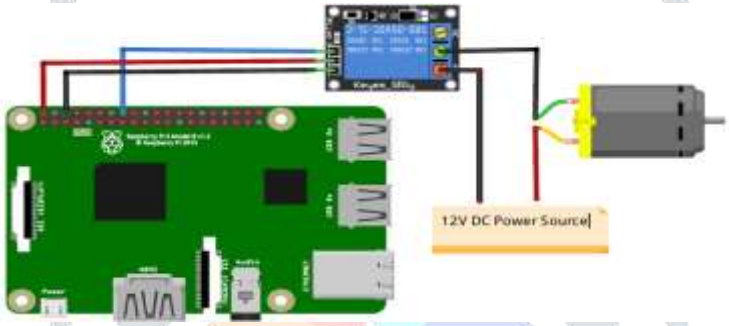

Fig4: Home security System with Face Recognition based on Convolution Neural Networks.

5. CONCLUSION

The automatic security system that is recommended is affordable and consumes minimal electricity. Because it utilizes IoT, the proposed system is effective and suitable for real-time applications. In our proposed system, the accuracy rate is about 95%. Because the system is constructed on WAN, the owner may view and control it from a distance. This system enables remote control and monitoring. The scheme's auxiliary components can be easily changed without affecting the settings. This configuration can be used in both online and offline settings. In order to stop fraud, the financial system may someday use debit cards, individual companies, and IoT-based security solutions. This system also has the ability to be merged.

6. REFERENCES

1. United Nations Office on Drugs and Crime(2017).https://dataunodc.un.org/crim/ Patel, K.K., Patel, S.M.: Internet of Things-IOT: definition, characteristics, architecture,enabling technologies, application & future challenges. Int. J. Eng. Sci. Comput. 6(5), 1–2 (2016)
2. Patibandla, R. S. M. L., & Narayana, V. L. (2021). Computational intelligence approach for prediction of COVID-19 using particle swarm optimization. In Advances in Computational Intelligence and Data Analytics (Vol. 923, pp. 175–189). Springer. https://doi.org/10.1007/978-981-15-8534-0_9

3. Santhi Sri, K., Sandhya Krishna, P., Lakshman Narayana, V., & Khadherbhi, R. (2021). Traffic analysis using IoT for improving secured communication. In Advances in Intelligent Systems and Computing (Vol. 213, pp. 499–507). Springer. https://doi.org/10.1007/978-981-33-4443-3_48
4. Narayana, V. L., & Bharathi, C. R. (2019). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs. In Advances in Intelligent Systems and Computing (Vol. 104, pp. 649–658). Springer. https://doi.org/10.1007/978-981-13-1921-1_63
5. Narayana, V. L., & Bharathi, C. R. (2018). Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS. Mathematical Modeling of Computer Systems, 91(2), 73–76. https://doi.org/10.18280/mmc_a.910207
6. Lakshman Narayana, V., Lakshmi Patibandla, R. S. M., Pavani, V., & Radhika, P. (2023). Optimized nature-inspired computing algorithms for lung disorder detection. In Advances in Intelligent Systems and Computing (Vol. 1066, pp. 103–118). Springer. https://doi.org/10.1007/978-981-19-6379-7_6
7. Narayana, V. L., Sudheer, B. N., Maddumala, V. R., & Anusha, P. (2020). Fuzzy base artificial neural network model for text extraction from images. Journal of Critical Reviews, 7(6), 350–354. https://doi.org/10.31838/jcr.07.06.61
8. Narayana, V. L., Bhargavi, S., Srilakshmi, D., Annapurna, V. S., & Akhila, D. M. (2024). Enhancing remote sensing object detection with a hybrid Densenet-LSTM model. In Proceedings of the International Conference on Computer Science and Advanced Technology (pp. 264–269). IEEE. https://doi.org/10.1109/IC2PCT60090.2024.10486394
9. Narayana, V. L., Syamalatha, P., Vatsalya, P., Sricharitha, V., & Akhila, V. (2023). Multi-level node authorization using recurrent neural networks for secure health monitoring system. Proceedings of the IEEE International Conference on Smart Computing and Networking Applications (ICSNA), 1697–1705. https://doi.org/10.1109/ICSCNA58489.2023.10370543
10. Gopi, A. P., Swathi, V., Harshitha, G. S., Swetha, B., & Alekhya, N. (2023). Prediction of paddy yield based on IoT data using GRU model in lowland coastal regions. In Proceedings of the 5th International Conference on Smart Systems and Inventive Technology (ICSSIT 2023) (pp. 1747-1752). https://doi.org/10.1109/ICSSIT55814.2023.10060935
11. Arepalli, P. G., Naik, K. J., & Amgoth, J. (2024). An IoT-based water quality classification framework for aqua-ponds through water and environmental variables using CGTFN model. International Journal of Environmental Research, 18(4), Article 73https://doi.org/10.1007/s41742-024-00625-2
12. Gopi, A. P., Babu, E. S., Raju, C. N., & Kumar, S. A. (2015). Designing an adversarial model against reactive and proactive routing protocols in MANETs: A comparative performance study. International Journal of Electrical and Computer Engineering, 5(5), 1111-1118. DOI: 10.11591/ijece.v5i5.pp1111-1118
13. Sravanthi, G. L., Devi, M. V., Sandeep, K. S., Naresh, A., & Gopi, A. P. (2020). An efficient classifier using machine learning technique for individual action identification. International Journal of

Advanced Computer Science and Applications, 11(6), 513-520. DOI: 10.14569/IJACSA.2020.0110664

14. Gopi, A. P., Durga Mani, P., Chandana, V. B., Sulthana, S. R., & Parameswari, P. P. K. (2024). Classification of fake news using enhanced capsule neural network. In 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation, IATMSI 2024. DOI: 10.1109/IATMSI60426.2024.10502837
15. Arepalli, P. G., & Khetavath, J. N. (2023). An IoT framework for quality analysis of aquatic water data using time-series convolutional neural network. Environmental Science and Pollution Research, 30(60), 125275-125294. https://doi.org/10.1007/s11356-023-27922-1
16. Gopi, A. P., & Jairam Naik, K. (2021). A model for analysis of IoT based aquarium water quality data using CNN model. In 2021 International Conference on Decision Aid Sciences and Application, DASA 2021 (pp.976-980). https://doi.org/10.1109/DASA53625.2021.9682251
17. Roshini, P., Khajavali, S., Snigdha, M. L. S., Harsha, B. D., Srilakshmi, B., & Gopi, A. (2024). CNN design with AlexNet algorithm for diagnosis of diseases in cassava leaves. In Proceedings - 2024 International Conference on Expert Clouds and Applications, ICOECA 2024 (pp. 711-718). https://doi.org/10.1109/ICOECA62351.2024.00129
18. Narayana, V. L., Gopi, A. P., Khadherbhi, S. R., & Pavani, V. (2020). Accurate identification and detection of outliers in networks using group random forest methodology. Journal of Critical Reviews, 7(6),381-384. https://doi.org/10.31838/jcr.07.06.67
19. Rao, B. T., Patibandla, R. S. M. L., Narayana, V. L., & Gopi, A. P. (2021). Medical data supervised learning ontologies for accurate data analysis. In Semantic Web for Effective Healthcare Systems (pp. 249-267). https://doi.org/10.1002/9781119764175.ch11
20. Patibandla, R. S. M. L., Gopi, A. P., Narayana, V. L., & Rao, B. T. (2023). Decentralized smart healthcare systems using blockchain and AI. In Blockchain applications in healthcare: Innovations and practices (Vol. 1, pp. 139-154). DOI: 10.1002/9781394229512.ch8
21. Lakshman Narayana, V., & Gopi, A. P. (2020). Enterotoxigenic Escherichia coli detection using the design of a biosensor. Journal of New Materials for Electrochemical Systems, 23(3), 164-166. DOI: 10.14447/jnmes.v23i3.a02
22. Narayana, V. L., & Gopi, A. P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34, 197-208. DOI: 10.3166/ts.34.197-208
23. Arepalli, P. G., Narayana, V. L., Venkatesh, R., & Kumar, N. A. (2019). Certified node frequency in social network using parallel diffusion methods. Ingenierie des Systemes d'Information, 24(1), 113-117. https://doi.org/10.18280/isi.240117
24. Peda Gopi, A., & Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4), 175-181. https://doi.org/10.3166/TS.34.175-181
25. Narayana, V. L., Gopi, A. P., Anveshini, D., & Lakshmi, G. V. V. (2020). Enhanced path finding process and reduction of packet droppings in mobile ad-hoc networks. International Journal of Wireless and Mobile Computing, 18(4), 391-397. https://doi.org/10.1504/IJWMC.2020.108539

26. Challa, R., YAMPARALA, R., KANUMALLI, S. S., & KUMAR, K. S. (2020, November). Advanced patient's medication monitoring system with ardunio UNO and NODEMCU. In 2020 4th International conference on electronics, communication and aerospace technology (ICECA) (pp. 942-945). IEEE.
27. Kanumalli, S. S., Chinta, A., & Chandra Murty, P. S. R. (2019). Isolation of Wormhole Attackers in IOV Using WPWP Packet. Revue d'Intelligence Artificielle, 33(1)
28. Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2018). Advances in Modelling and Analysis B. Journal homepage: http://iieta. org/Journals/AMA/AMA_B, 61(1), 5-8.
29. Kosaraju, Chaitanya, et al. "A model for analysis of diseases based on nutrition deficiency using random forest." 2022 7th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2022.
30. Chaitanya, Kosaraju, and Gnanasekaran Dhanabalan. "Secure Route Detection with Multi Level Trust Evaluation Model Using Replicated Auditor Node for Extended Packet Delivery Rate in WSN." Revue d'Intelligence Artificielle 37.4 (2023).
31. Chaitanya, Kosaraju, et al. "Risk Stratification for Stroke Using Attention Transformer Model." 2024 2nd International Conference on Disruptive Technologies (ICDT). IEEE, 2024.
32. Prasanna, K.L., Niharika, K., Charishma, V., Sai, K.B.,K(23),"Network Intrusion Detection using Deep Reinforcement Learning,**Proceedings - 7th International Conference on Computing Methodologies and Communication", ICCMC 2023**, 2023, pp. 1146–1150
33. Sunitha, Anitha, B.S., Rama, G.T., Niharika, N., Sahithi, A.,K(23),"Convolutional Neural Network (CNN) based Blood Vessel Segmentation from Ocular Images**Proceedings - 7th International Conference on Computing Methodologies and Communication**",**ICCMC 2023**, 2023, pp. 518–523
34. Majety, V. D., & Murali, G. (2018). Remote health watchdog framework for seizure patient using electronic sensors. International Journal of Engineering and Technology(UAE, 7, 783–785. https://doi.org/10.14419/ijet.v7i3.12132
35. Alapati, N., Anusha, N., Joharika, P., Jerusha, N.J., Tanuja, P.(2023)Prediction of Parkinson's Disease using Machine Learning in 2023 2nd International Conference on Electronics and Renewable Systems(ICEARS)(pp.1357–1361).IEEE
36. 36.Naresh, A., Reddy, B.A., Reddy, G.P., Kumari, K.R., Vaishnavi, M.S.(2023)Melanocytic Pigmented Skin Lesion Detection and Classification using Hybrid Deep Features based on Fully Convolutional Network in 2023 2nd International Conference on Electronics and Renewable Systems(ICEARS)(pp.1011–1018).IEEE
37. Pavani, Vellalacheruvu, and I. Ramesh Babu. "Three level cloud storage scheme for providing privacy preserving using edge computing." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1929-1940.
38. Vellalachervu, Pavani and Babu, I. Ramesh, A Novel Method to Optimize the Computation Overhead in Cloud Computing by Using Linear Programming (May 10, 2019). INTERNATIONAL JOURNAL

OF RESEARCH AND ANALYTICAL REVIEWS(IJRAR), May 2019, Volume 6, Issue 2,AvailableatSSRN: https://ssrn.com/abstract=3452191

39. Rama Krishna, Komanduri Venkata Sesha Sai, and Battula Bhanu Prakash. "Intrusion Detection System Employing Multi-level Feed Forward Neural Network along with Firefly Optimization (FMLF2N2)." Ingénierie des Systèmes d'Information 24.2 (2019).
40. Krishna, K. VSS Rama, et al. "Identification of Fraud Transactions using Lightgbm Technique." 2022 3rd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). IEEE, 2022.
41. S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1260-1268, doi: 10.1109/ICEARS53579.2022.9752280.
42. Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1916-1928.
43. Qi, Zhang, P. SilpaChaitanya, and T. Sudhir. "Spoofing attack detection wireless networks using advanced KNN." International Journal of Smart Device and Appliance 4.1 (2016): 1-8.
44. S. K. P, J. Lavanya, G. Kavya, N. Prasamya and Swapna, "Oral Cancer Diagnosis using Deep Learning for Early Detection," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022,pp.1260-1268, doi:10.1109/ICEARS53579.2022.9752280.
45. Krishna, P. Sandhya, SK Reshmi Khadherbhi, and Vellalachervu Pavani. "Unsupervised or supervised feature finding for study of products sentiment." International Journal of Advanced Science and Technology 28, no. 16 (2019): 1916-1928.
46. Sharmila, S., & Aparna, C. (2019). VMSSS: A proposed model for cloud forensic in cloud computing using VM snapshot server. In Advances in Intelligent Systems and Computing (Vol. 816, pp. 483–493). https://doi.org/10.1007/978-981-13-1592-3_38
47. Mohiddin, S.K., Sharmila, S., & Srinivas, V. (2024). Intelligent transport system in smart cities: Aspects and challenges of vehicular networks and cloud computing. In Energy Efficient Vehicles: Technologies and Challenges (pp.173–185). https://doi.org/10.1201/9781003464556-9
48. Mohiddin, S.K., Sharmila, S., & Sharma, V. (2024). Wireless technology for providing safety in VANETs. In Wireless Communication Technologies: Roles, Responsibilities, and Impact of IoT, 6G, and Blockchain Practices (pp. 19–35). https://doi.org/10.1201/9781003389231-2
49. Sharmila, S.K., Nikhila, M., Lakshmi Prasanna, J., Lavanya, M., & Bhavana, S. (2023). Unique web-based assessment with a secure environment. Lecture Notes in Networks and Systems, 673, 725–736. https://doi.org/10.1007/978-981-99-1745-7_53
50. Chin, H.: Face recognition based automated student attendance system. Diss. UTAR (2018)
51. Senthilkumar, G., Gopalakrishnan, K., Kumar, V.S.: Embedded image capturing system using raspberry pi system. Int. J. Emerg. Trends Technol. Comput. Sci. 3(2), 213–215 (2014)
52. Sowmiya, U., Mansoor, J.S.: Raspberry pi based home door security through 3G dongle. Int. J. Eng. Res. Gener. Sci. 3, 138–144 (2015)