Artificial Intelligence Based Person Identification Virtual Assistant

P.Praddeep, P.Balaji, S.Bhanumathi

x

Abstract: In future all the electronic gadgets are operated by usingvirtualassistantwhichisanythingbutdifficulttogettoyetit needs in security. Project aims to provide security for virtual Assistant (VA) through facial recognition. The framework enables just approved users to access voice commands. By this we can get protection and security for virtual assistant (VA). Users can ask their help addresses like time, date and climate and find solution to the inquiries. This virtual assistant causes us to send email through voice commands and it also takes notes from voice commands with security. It gives access to the unapproved user to enlist with the required consent from the administrator. It is can exchange the pictures and documents just by using voice commands. It will take photographs using camera when we use the fitting voice commands. Various users in a family can get access to the virtual Assistant by facial recognition module.

Index Terms: Virtual Assistant, Facial Recognition and Security.

I. INTRODUCTION

In Today's advanced crisp market for artificialintelligence could be a key unlocking the users of tomorrow. Man-made brainpowerisasofnowallaroundtheuser.Manydependon it every day as per Gartner about 38% of consumers have utilized virtual assistant benefits on their smart devices as of late numerous enterprises receiving AI to convey the logical conversationalconsistent and customized home administrations now is the ideal time to be natural and proactiveabouthowuserswillencounteritandcrossoverany barrier between the innovation and how it helps users are devouring it then AI gets advanced with power huge information and investigation it can offer a one of a kind and separate clientexperience.

Users like to associate with the machines using voice commands which are conceivable through the virtual assistant,gadgetsforexample,smartphones,smartTV' s and car navigation systemsandsoforth.Thevirtualassistantsare the astute operators that can enable userstocomplete [13].

Undertakingmoresuccessfullyandadvantageouslybymeans ofspokencollaborationsamonguserandthevirtualassistant.

Thevirtualassistantscansupportawidescopeforallusersin business enterprises, education, government, medicinal services and diversion. The main organizations planned their own virtual assistants, for example, Microsoft's Cortina, Apple'sSiri,Amazon'sAlexaSamsungSVoice,andGoogleAssistant. Generally, these collaborators have these normal highlights like programmed automatic speech recognition,

Text to speech, manufactured talking face and dialog management [4,14].

The virtual assistant is improved by giving Facial Recognition framework. The facial recognition framework forvirtualassistantusingAIstrategiestodetectandrecognize faces. They are two kinds of users like approved clients and unapproved users [2]. The user stands before the camera which takes different pictures of the user. The captured pictures experience the face detection process [12]. In this procedureitidentifiesfacesinthepicturesandenablesaccess to the virtual assistant for the approvedusers.

II. RELATEDWORK

The author in [1] presented about the attacks to voice assistance, that can be followed in a several availabilities which are given in several operating systems attackers can principally control these apparatuses to perform unapproved commands. The assailants could release the delicate datalike user's area visit web pages which contain malware to gain unapprovedaccesstocertaingadgetsthispromptsspillageof touchydata.

Voice assistance can be utilized without getting any permission from the user. Voice assistance attacks are generally static attacks, attackers broadly utilize recorded sound documents which are played by applications or by staticmediumthismaycausesendingmailsandsesamevoice calls

Even send post via web-based networking media aggressors can utilize voice help for long range interpersonal communication applications to post destructive things from user account.

At times the voice recognition may fail by getting great exampleofvictim'svoiceandutilizepreparedvoiceengineto copy his voice. The usage of a voice order framework as an Intelligent Personal Assistant (IPA) can play out various errands or administrationsfora person. In this framework one can make inquiries to the framework,conjureitsAIgenerallygetitfromWikipedia[2].

Theauthorsinthe[4]proposedthatinsight full projectswith natural language processing that are as of nowaccessible,with various classifications of support, and look at the helpfulness of one explicit bit of programming as a Virtual Personal Assistant. Which are analyzed by fundamental regular language handling and the capacity to work without the requirement for other sort of human info (or

Revised Version Manuscript Received on 10 September, 2019.

Penumarthi Pradeep, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, pradeep.proton@gmail.com.

Pallapothu Balaji, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, pallapothu96@gmail.com.

S.Bhanumathi,School of Computing, Sathyabama Institute Of Science and Technology, Chennai,banujun8@gmail.com.

Retrieval Number: B12590982S1119/2019©BEIESP
DOI: 10.35940/ijrte.B1259.0982S1119

programming) may as of now be reasonable in the menial helpers however at some point it might fail because of prepared voice engine to mirror his voice.

III. EXISTINGSYSTEM

Virtualassistancecandoanythingwithoutanindividualfor help. VA can do administrative assistance like sending email and taking notes.VA can access the information form online website and gives information to the users. This information can be extracted in Jason and converted into text format this text format again converted into speech. This system will interact with the user and fetched information form online cloud according to the question asked from the user. voice activateddigitaldeviceslike amazon choandpersonalAlexa assistant may also raise personal concerns like amazon is considering giving trance scripts Alexa's audio recordings to the third-party. When they hear key word Alexa, they start recording the voice which is not necessary. This recording was stored in the developer's database. As artificial intelligence is based on data and data is based on the recordings of theusers.

IV. PROPOSEDSYSTEM

TheFacialRecognitiontothevirtualassistantgivesgreater security to the system by the Haar Cascade algorithm. The face is recognized by the camera and it is handled through OpenCV in which it detects the faces and articles placed put before the the cameraandthepicturestakeniscontrastedwith the pictures in the in the system by Haar Cascade Algorithm. After recognizing the face it permits to interact with the virtualsystem.

The virtual assistant hangs tight for our voice commands. Heretothevirtualassistanttheinputisgiveninspeechformat throughBluetoothconnecteddevicethensystemconvertsthe speech in to the text format and understands the input and undergoes processing and gives the appropriate output in the text format later it is converted to speech format as outputby theuseofeSpeak(speechsynthesizer)andtheoutputisinthe audio format.

FACEDETECTION:

Createadatabaseinwhichallthetrainingimagesarestored and all the images are captured by the camera are stored in database. The face recognition is finished by using two algorithmstobespecificHaarCascadeAlgorithmandFisher Face Algorithm. In the Haar Cascade algorithm is based on Cascade classifiers which consists of haar features. The cascade classifiers are the concatenation of a set of weak classifiers used to create a strong classifier. These classifiers identify the human face dependent on the most significant highlights like eyes, eyebrows and lips. Haar features are detected based on the concrete computation, in which we allocate a pixel intensity to every single pixel related to grayscale values inside the scope of 0 to 255 where 0 speaks to the white shading and 255 speaks to the darkshading.

0.2	0.3	0.7	0.7
0.1	0.1	0.8	0.6
0.1	0.3	0.6	0.8
0.1	0.2	0.7	0.5

Fig 4.1: original values detected on an image.

0	0	1	1
0	0	1	1
0	0	1	1
0	0	1	1

Fig 4.2: Ideal Haar features and Pixel intensities 0 for white and 1 for black.

FACERECOGNITION:

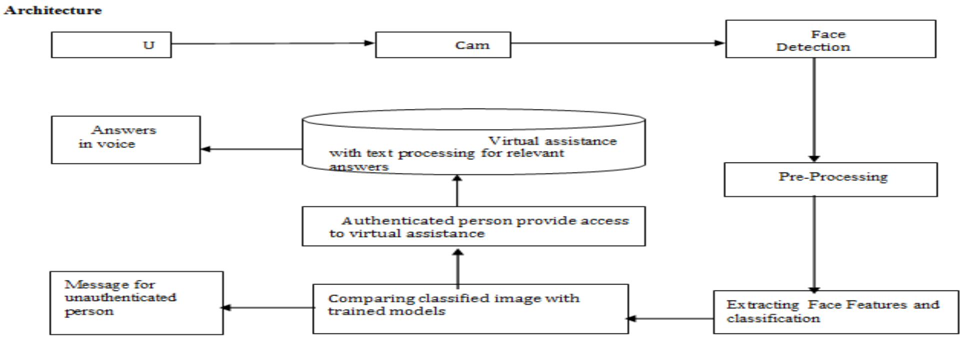

Architecture
U
Cam
Face Detection
Answers in voice
Virtual assistance with text processing for relevant answers
Pre-Processing
Authenticated person provide access to virtual assistance
Message for unauthenticated person
Comparing classified image with trained models
Extracting Face Features and classification

Fig 4.3 Person Identification VirtualAssistant

Inthefig5.3cameracapturesthephotooftheuserandthen ittrainsthemodelsfortheimagesstoredinthedatabasewith respective to the features of the person. In the detection sectionitdetectsthefacebasedonthehaarxmlfilewhichhas some pre-defined features of face. After detecting the face, it will start extracting the features of the face. By considering the features the images are classified accordingly. These classified images are compared with the trained models. If it matches the user can access the virtualassistance.

4.1.2 RECONIZING THE DETECTEDFSCE:

InFisherfaceAlgorithmthepictureswhichareavailablein c number of classes with n samples for every individual dataset and it is given as the example set of K's the place K ranges from 1 to c and every individual sample of T has the scope of 1 ton.

K={K1,K2,… ,Kc}[11]

Ki={k1,k2,… ,kn}[11]

To acquire the global mean of the considerable number of pictures and all the class this characterized by μ and μi is the meanofpictureswithineachclass.Toacquirethechangeand

Ascertain the variance matrix which helps us to gives the scatter inside the class. For each class discover the contrast between the picture and the mean esteem which is related to class where the picture adjusted.

Sw=∑Cj=1∑nji=1(xij−μj)(xij−μj)T [11]

Wherexijistheithtestofclassj,μjisthemeanofclassj , and nj the quantity of tests in class j ,Sw is the scatter within theclass

The scattering between the classes is determinedutilizing Sb=∑Cj=1(μj−μ)(μj−μ)T[11]

Where Sb is the scatter between the classes.

We now need to discover those premise vectors V where Sw is limited and Sb is augmented, where V is a network whose sections vi are the premise vectors characterizing the subspace. These are given by,

|VTSbV||VTSwV| [11]

The answer for this issue is given by the summed up eigen value decay.

SbV=SwVΛ, [11]

V. IMPLEMENTATION

Necessary packages

- Bluetooth
- Time
- Httplib
- urllib2
- json
- subprocess
- cv2
- Sys
- numpy
- os
- subpocess

CreateDatasets

The accompanying advances will make the datasets this is finished utilizing haar cascade frontal face default xml file trained features of faces.

1. Make an informational index envelope with the end goal that every one of the countenances to be perceived results in these present circumstancesorganizer.

2. Instate the Hight and width of the face that is taken while catching thepicture.

3. Import the haar record utilizing openCV open source application which has some pre-characterizedcapacities.

4. OpenCv helps us to utilize webcam with the assistance of VideoCapturefunction.Ontheoffchancethat0ispassedas thecontentioninthiscapacityitwillutilizewebcamofthePC else 1 is passed which initiates different cameras which are associated with thegadget.

5. To take n quantity of pictures loop the functions readfrom webcam and cvt.color which changes over shading to high contrastofcourseuseloopcommandinsidetheloopforeach and every coordinate offace.

6. Inside this nested loop actualize factions of the OpenCV rectangle shape in which picture caught by the camera, arranges and shading range is given asarguments.

7. To detect the face use function face_cascde.detectMultiScale with gray and cascade values are given as arguments and use resize and image the write faction for resizing theimage.

FaceDetection

For Face detection we use Haar Cascade algorithm which involves in the following steps:

1.

In the Haar Cascade algorithm is based on Cascade classifiers which consists of Haar features which are in Haar file helps for the detection of theface.

2. Thecascadeclassifiersarethecombinationofasetofweak classifiers used to create a strongclassifier.

3. This combination forms a triangle shape which consists of black and white identification lines onthe

Face is recognized using the fisher facealgorithm:

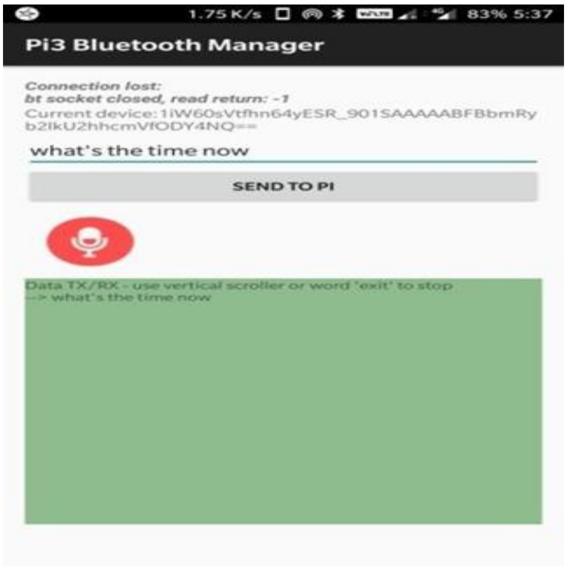
This involves in two parts. They are Creating Fisher Recognizer and to use Fisher Recognizer on the camera stream.

Part1:Thisinvolvesintrainingtheimagesinwhicharestored in the datasets. Create two lists which consist of images and their corresponding names. Loop the image and their id for each and every subdirectory in the dataset. Then create a numpyarraycommonforboththelists.OpenCvhelpstotrain models for images with respective their id using train function.

Part 2: In this the Fisher Recognizer helps to recognize the face on camera stream. First it will detect the face in front of thecamerausinghaarfile.Thedetectedfaceisconvertedinto black and white image. Use gray and resize functions for modification of the capturedimage.Thetrainedmodelgivesthepredictionvaluefort hecaptured image the minimum limit of the prediction value is five hundred.Ifthepredictionvalueislessthanfivehundredthen thepersonisauthenticatedelsethepersonisunauthenticated.

Get Access to VoiceCommands

Ifthepersonisauthenticatedthenheorshewillgetaccessto voicecommands.



1.75 K/s 83% 5:37

Pi3 Bluetooth Manager

Connection lost:
bt socket closed, read return: -1
Current device: 1iW60sVtfhn64yESR_901SAAAAABFBbmRy b2lkU2hhcmVfODY4NQ==

what's the time now

SEND TO PI

Data TX/RX - use vertical scroller or word 'exit' to stop
--> what's the time now

Fig 5.1: Flow of Face Recognition Virtual Assistance.

This voice commands are revived via Bluetooth connection through a socket bind with port 1. The socket connection is automatically connected to the virtual assistant if we add the device in the Bluetooth module of the virtual assistant. The received data through attachment was examined through conditions given and offer response to the regarded individual.

For the appropriate responses that ought to be replayed is finished by bringing in Wikipedia and wolfram alpha. Wikipedia will give the responses for the general questions and wolfram alpha will give responds to for the intelligent inquiries. Utilizing voice commands, the virtual assistantcan write notes and send email through the SMTP server. It likewise gives answers for climate, date, time and takes photographs of thepeople.

Flow Chart for face Recognition VirtualAssistance

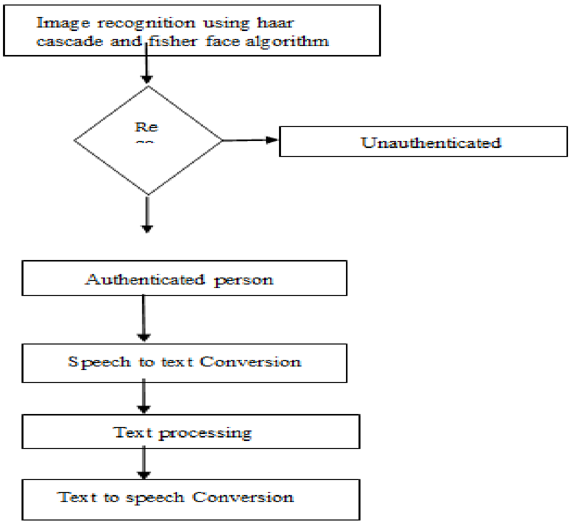
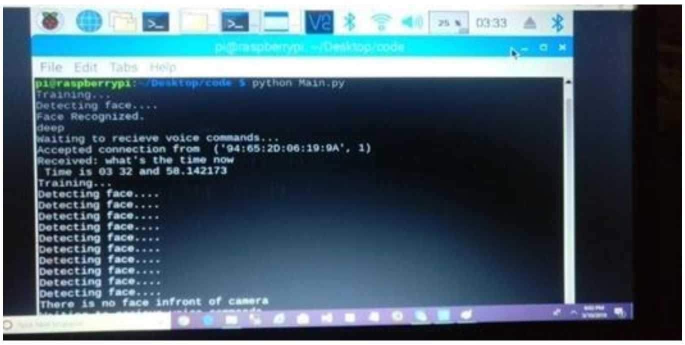


Image recognition using haar cascade and fisher face algorithm
Re --
Unauthenticated
Authenticated person
Speech to text Conversion
Text processing
Text to speech Conversion

Fig 5.2 Flow of Face Recognition Virtual Assistance.

In the flow chart of fig.5.1 the recognition part takes place first which leaves two possibilities of a person getting authenticated and unauthenticated. If the person is unauthenticated it stops the process and get back to its initial position where as in case of authenticated person it follows the procedure flow. The speech given by the person is converted into the text format which would be getting processed in the next step. Then finally the processed text isfollowedwiththeresponsegivenbythemoduletothespeech form.Thisishowthefacerecognitionvirtualassistancetakes place.

VI. RESULTS



```
pi@raspberrypi:~/Desktop/code $ python Main.py
Training...
Detecting face....
Face Recognized.
deep
Waiting to recieve voice commands...
Accepted connection from  ('94:65:2D:06:19:9A', 1)
Received: what's the time now
 Time is 03 32 and 58.142173
Training...
Detecting face....
Detecting face....
Detecting face....
Detecting face....
Detecting face....
Detecting face....
Detecting face....
Detecting face....
Detecting face....
Detecting face....
There is no face infront of camera
```

Fig 6.1 Face Input for Authentication The Virtual Assistance.

In the fig 5.3 cameras captures the photo of the user and then it trains the models for the images stored in thedatabase with respective to the features of the person. In the detection sectionitdetectsthefacebasedonthehaarxmlfilewhichhas some pre-defined features of face. After detecting the face, it will start extracting the features of the face. By considering the features the images are classified accordingly. These classified images are compared with the trained models. If it matches the user can access the virtualassistance.

The input is taken in the form of picture as shown in the figure 6.1. This input is processed with the trained models. There are usually three scenarios when it is processed with trained models namely:

1. authenticated person.
2. Unauthenticated person.
3. thereisnofaceinfrontofthecamera'commentforthe third case of not having input face at the cameravision.

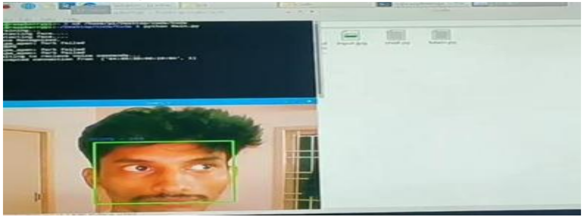


Fig 6.2: Output for the detected Face and Replay for Questions.

Incaseofauthenticatedpersonitwouldhavetheaccesstothe virtualassistancethroughwhichwegivetheinputintheform ofmethodologyusedinfig.5.1.Itaswellasgivetheresponse to the questions asked by theperson.

Incaseofunauthenticatedpersonitleavesamessageandgoes backtoitsrecognitionpartofitsloopinanykindofscenario.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

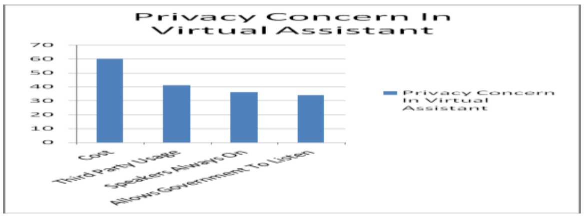
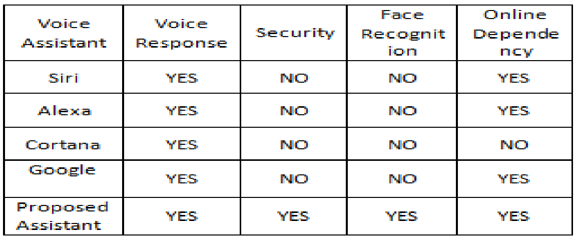


Fig 6.3 Privacy and Security Issues Faced ByVirtual Assistants.

Thebarchatsinfig6.2frepresentstheprivacyandsecurity issues faced by the virtual assistants. In the year 2017 forty one percentage of the virtual assistance was used by third party. The virtual assistance is always active results in recordingsensitiveinformation.Someasthesecuritypurpose government will listen to our private conversation all this problems can be resolved using face recognition. This may solve by voice recognition but the attackers uses recoded mimic voice and get access for the virtual assistance. This show the need of security in the virtualassistant.

Table 6.1 Represents Several Voice Assistants and their features and How it differs from Proposed Model



Voice Assistant	Voice Response	Security	Face Recognition	Online Dependency
Siri	YES	NO	NO	YES
Alexa	YES	NO	NO	YES
Cortana	YES	NO	NO	NO
Google	YES	NO	NO	YES
Proposed Assistant	YES	YES	YES	YES

In the table 6.1 represents the several voice assistants including proposed assistant accessibilities in the various fields. All the assistant's response to the audio input whichis known as voice response, The Google Assistant and Siri can be activated when the screen is locked whereas other assistants lacks this feature. Proposed Assistant has Facial recognition that enables more security. Proposed system can sendmailinmoresecuredwaythantheothervoiceassistants.

VII. CONCLUSION

This paper will help to demonstrate that virtual assistant is attackedbythirdpartyandgivesasolutiontotheproblem.In this the virtual assistant is improvised with Facial Recognition. The facial recognition system for virtual assistant using Machine learning strategies to detect and recognize faces. After recognizing the face, the users can access the virtual assistant. If the person is third party ten it will say unauthenticated person. The unauthenticated person can get access to virtual assistance with administer permission. This Assistance can send email and take notesof some personal information only for the authorized person it also says some general information like time, date and weather.

REFERENCES

1. Efthimios and Constantino in 2017, "Monkey says, Monkey Does-Security and Privacy on VoiceAssistants", IEEE journal, ISSN: 2169-3536.
2. Peter Imrie and Peter M.Bednar, 2013, "VirtualPersonal Assistant" in Research gate with ISBN: 978-88-6685-007-6 4.
3. Emad S. Othman in November 2017, "Voice Controlled PersonalAssistantUsingRaspberryPi",InternationalJournal of Scientific & Engineering Research Volume 8, Issue 11, 1611, ISSN2229-5518.
4. Anurag Mishra, Pooja Makula, AkshayKumar,Krit Karan and V. K. Mittal, May 28-30, 2015, "A Voice-Controlled Personal Assistant Robot", IEEE journal, Page: 8, INSPEC accession number 15291099.
5. Tatiana Ekeinhor-Komi, Jean-Léon Bouraoui, Romain Laroche, Fabrice Lefèvre, 09 February 2017, "Towards a virtual personal assistant based on a user-defined portfolioof multi-domain vocal applications", IEEE Xplore, INSPEC 16657478.
6. O.Portillo-Rodriguez,C.A.Avizzano,A.Chavez-AguilarM. Raspolli, S. Marcheschi and M. Bergamasco, "Haptic Desktop: The Virtual Assistant Designer", IEEE/ASME International Conference on Mechatronics and Embedded Systems and Applications.
7. Bisma Shakeel, Tabasum and Mir Shahnawaz Ahmad in July- 2017, "Siri - Apple's Personal Assistant: A Review", International Journal of Computer Science and Mobile Computing ol.6 Issue.7, ISSN2320-08.
8. Sanchez, Carlos, Mun˜oz de la Pen˜a, David, Gomez-EsternandFabio,"Virtualassistantforindividualized practical training on controller desig", ScienceDirect, IFAC 48 29 2015 205210.
9. Prajyot Mane, Shubham Sonone, Nachiket Gaikwad and Jyoti Ramteke, "Smart Personal Assistant using Machine Learning", International Conference on Energy, Communication, Data Analytics and SoftComputing,ICECDS-2017.
10. Hyung-Ji Lee, Wan-Su Lee, and Jae-No Chung, 2001 published their paper "Face Recognition Using Fisherface Algorithm And Elastic GRAPH Matching", IEEE withISBN 0-7803-6725-1.
11. Sushma Jaiswal, Sarita Singh Bhadauria and Rakesh Singh Jadon, July 2011, "Comparison Between Face Recognition Algorithm-Eigenfaces, Fisherfaces And Elastic BunchGraphMatching",Volume2,No.7,JournalofGlobal Research in Computer Science,ISSN-2229-371X.
12. Dr.R.Subhashini, E.Nagarajan and Niveditha.P.R, "Detection Of An Incognitos Intruder in Industries and Semantic Mapping Of Emotions", International Journal Of Applied Engineering Research, ISSN-0973-4562, VOLUME 9, Number 20(2014) pp.6727-6734.
13. R.Subhashini and V. Jawahar Senthil Kumar, "Shallow NLP Techniques for Noun Phrase Extraction", Presented in the International Conference on Trendz in Information Sciences & Computing (TISC - 2010) in association with Cognizant Technology Solutions and IEEE from 17th to 19th of December, 2010, Sathyabama University, Chennai.

AUTHORS PROFILE

Penumarthi Pradeep, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, pradeep.proton@gmail.com.

Pallapothu Balaji, Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, pallapothu96@gmail.com.

S.Bhanumathi,School of Computing, Sathyabama Institute Of Science and Technology, Chennai,banujun8@gmail.com.