IoT in Safety and Security of Automobiles

Shamik Palit, Chandrima Sinha Roy

Abstract*: This article is about IoT. The IoT on vehicles will be discussed. For an automobile for safety and security, I am making progress in making an IoT comparative analysis. A new web wave that is expected to rework our lives could be the Things Web (IoT). The Web has people connected andconnects Things to create flawless communication and pooling of intelligence. IoT could be an era of RIOTous, with the remarkable ability to control the world and the method we tend to live. It uses gadgets and sensors relating to the net, which produce new characteristics. In the age of modern international, we as the purchasers are leaning in the direction of smart vehicles and extra to make lifestyle easier. The Internet and society center states that 90% of accidents that occur around the place are caused by human errors and failures. We can reduce the error from the very least when we implement IoT on cars. In 2020, the Automobile Manufacturers ' Alliance forecast that 75% of cars are capable of using the internet and that unsecured devices can be accessible without difficulty, which is why it is important that safety is guaranteed in cars. This paper analyzes the various securities of IoT technologies in IoT.Then suggesting new security policy

***Keywords*: Internet of Things, Safety, Security, Automobile.**

I. INTRODUCTION

A. Internet of Things

IoT is a giant connected device network. These devices collect and share information on how they are used and how they share the environment. IoT provides a platform for dumping and communicating with each other in a common language. For a broad definition:" It is a system of interrelated devices, machines, animals or people that provide a unique UID and transmit data through the wireless network.[1]

B. How IoT was discovered

The term Things ' internet is 16 years old. However, the real idea of connected devices was longer, at least since the1970s. The idea was often referred to as the " internet embedded " or " invasive computing. " However, in 1999, during his work in Procter&Gamble, Kevin Ashton coined the actual term " Internet of Things. " Ashton, who worked on optimizing the supply chain, wanted to Calling theattention of the senior management to a new exciting RFID technology. Since the Internet was the hottest new trend in 1999. *he called hispresentation"TheInternetofThings,"as*it was somehow meaningful. Although Kevin took the interest of certain P&G managers, the word Internet of Things, for the next 10 years was not widely used [2]. By 2013, the Internet of Things had evolved into a multi-tech system ranging from the Internet, WLAN communication, and micro-electromechanical (MEMS) systems, to embedded systems. IoT is supported by traditional automating systems (including building and home automation), wireless sensor networks, GPS, monitoring devices, etc. The Internet of Things is a device that is simply indicated with an Internet connection on / off switch. This comprises almost anything, from mobile phones to the maintenance of buildings to the jet engine of an avion. Medical devices like implants with a heart monitor or a biochip transponder in a farm animal, can transfer data over a network and are members The IoT' s. If it does have an off / on switch, it can be part of the system theoretically. The IoT comprises a huge network of " things" and devices connected to the internet. An excellent example of a recent addition to the Internet of Things is Ring, which links to your smartphone. You can see who it is and speak with it when you press the doorbell, Ring[3].

C. Architecture of IoT

ThearchitectureofIOTcanbevariedfromtheanswertoanswerw hereinwhichwewanted to build it. It can be consists of four main components where these can be framed.

The first and the foremost layer comes to the sensors/actuators. Sensors will be taking the data from the environment and turning them into useful data. Actuators will be involving to changing the physical data to generate the data.

The second will be the Sensors/Actuators Data Acquisition systems. They will be sitting near to the sensors and actuators. Like we can take an example where a pump will have a half dozen sensors and actuators that will put the information into the information collecting device which will digitize the data. They will be attached to the pump. A gateway device would process the data and move it to the third and fourth.

Third is Edge IT. Once the data has been digitized and aggregated which will move from the world of IT. But the data will require further calculations before entering the data Centre. It will be performing more analysis. The IT processing systems will be located in remote offices which will generally sit in the facility.

The fourth will be the Datacenter. The data processed from stage three is moved to the physical data center where there will more powerful IT systems which can analyze, manage and secure the data. It will take a longer time to get answers where waiting is there until reaching stage.

Revised Manuscript Received on November 23, 2020.

***** Correspondence Author

Shamik Palit*, School of Engineering & Information Technology, Manipal Academy of Higher Education Dubai Campus, Dubai, United Arab Emirates. Email: shamik1980@gmail.com

Chandrima Sinha Roy,Department of Computer Science, Eminent College of Managementand Technology, Kolkata, West Bengal, India, Email: mail2chandrima@gmail.com

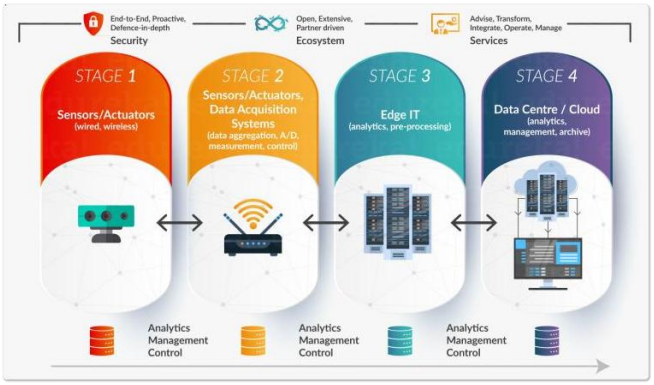

Fig 1: Architecture of IoT

D. Applications of IoT

Environmental Monitoring

IoTenvironmentalmonitoringapplicationstypicallyusesensors toprotecttheenvironment bymonitoringthequalityofairorwater,atmosphericorsoilconditions,includingwildlife and habitat surveillance areas. IoT devices typically cover a large geographical area inthis application and can also be mobile.

Transportation

The IoT can help integrate communication, control and information processing between different transport systems i.e., The driver, vehicle, infrastructure, or user. Dynamic interaction between these transport system components enables inter-and intra-vehicle communication, intelligent traffic control, smart parking, vehicle control and road and safety assistance.

Medical and Healthcare Systems

IoT devices can be used for remote health surveillance and emergency systems. These medical devices can range from blood pressure monitoring and heart rate monitoring to advanced devices, such as heart rate monitoring devices or advanced hearing systems, whichmonitorspecializedimplants.Specializedsensorscanalso bedesignedforthehealth and well- being of senior citizens in living areas.

Manufacturing

Manufacturingequipment,assetmanagement,andsituationmanagementormanufacturing process control and management of the network bring IoT to life for industrial and intelligent manufacturing. In order to optimize plant safety and security for process controls, operator tools, and service information systems, IoT automates digital control systems. It also extends to asset management to maximize reliability through predictive maintenance, statistical assessment, and measurements.

Building and Home Automation

IoT devices can be used in the monitoring and control of mechanical, electrical and electronic systems in various types of private, industrial, residential and institutional buildings. Home automation systems usually control lighting, heating, ventilation, air conditioning, equipment, communication, entertainment and home security equipment to improve comfort, energy efficiency, and safety.

II. PROBLEM DEFINITION & OBJECTIVE

A. Motivation

The driving forces and the benefits that drive me are increasingly severe, as IoT computer viruses are being increasingly used by agencies, industries and technicians. There can be a wide variety of IoT network connected devices. An estimate says that the quantity will reach almost forty billion, that is about 30 equipment for each and every animated consumer in the social community in the world. That's a prudent estimate. The IoT will include " trillions of sensors " another analyst predicts. Therefore, in the future, cars might be equipped with IoT connection gadgets and can have the complete detail of the car.

B. Problem

The problem is that in recent years, there has been an increasing volume of vehicles. The long established vehicle safety systems depend on numerous sensors and on the ever-high cost. There is no way to retrace the vehicle when the vehicle is stolen.

Figure 2: Motor Theft Statistics[4]

C. Objective

Authentication could be based entirely on a comparative assessment of IoT in cars. Since the arrival of cars, the car manufacturers wanted to make cars more secure and easier to drive.Itthereforerevolutionizeshumanbeingsfromonelocation toanotherbecauseofthe modern technology including IoT. While IoT is embedded in the car, mankind will adapt their ways of interacting with any vehicle equipment. The scope of IoT in the vehicle is extremely large and can be partially or maximally implemented in order to enhance the present day worldwide. The main objective or scope is to make use of,, reliable authentication technique. After that suggest a new security policy to the existing policy.

III. LITERATURE REVIEW

We can protect the car from external sources like theft by using IoT devices. Biometricsis theuseforidentificationandaccesscontrolofthebehavioralandphysicaldataobtainedby the individual and used for a number of existing technologies.

Biometrics is still an important part of driving technology development and devices such as iris scanners are expected to become a standard safety feature for unlocking and launching the vehicle [5]. Sayantam Sadhukhan, Arita Acharyya and Rajendra Prasad in their paper 'Car Security SystemusingFingerScannerandIoT'presentedanoblesystemto detectvehicletheft.The system memory is stored with fingerprints. The controller triggers the power circuit of the ECM, if the Fingerprint and RFID matches with the stored one. They did not speak much of the algorithm used but used gen2, GPS, GSSM, Wi-Fi module, and SD card. System also includes some other car burglary sensors. The owner of the fuses will benotified with GPSofthelocationofthecarwhentheburglartriestoactivatetheb atterywithpaperclips. So, together with GPS and RFID, they finalized a car fingerprint protection system.[6]

Hairol Nizam Mohd. Shah, Mohd. Zamzuri Ab Rashid, Mohd. Fairus Abdollah, MuhammadNizamKamarudin,ChowKokLinandZalinaKamis intheirpaper'Biometric Voice Recognition in Security System' presented a review on voice as A technology of biometrics. There are many methods in voice recognition, such as the Hidden Markov (HMM) Model, fusion classifiers system, dynamic time wrapping algorithm, and the Gaussian Mixture(GMM) Model, the latest being MATLAB vectorquantization.[7]

N.Kiruthiga,L.latha,S.Thangasamyintheirpaper'RealTime BiometricsbasedVehicle Security System with GPS and GSM Technology has presented an assessment using a bio metric technology, based on fingerprint. Here it mentions the algorithms that are in use. Here, when the person son places his finger on the fingerprint scanner, he registers. And protection is made in the higher end by ECU. So the user's fingerprint is a conclusion.[8]

Usha Rani J, Dr T H Sreenivas in their paper 'Remote Vehicle Tracking System through Voice Recognition App Using Smart Phone' presented a review based on voice as a biometrictechnology.Hereasimpleandreliablesystemhasbeen designedwhichwillgive an alert in the form of a text message as as any problem arises.The System will be using speechcommandssuchas'stop'etc.Sointheconclusionweobser vethatvoicecanbesue as a biometric system.[9]

IV. BACKGROUND

The internet of things (IoT) is the interconnected system of computing devices, mechanical or digital machinery, objects, animals or people which have unique identification (UID) and the ability to transfer data over a network without requiring human to human or human to computer interaction. At the same time, the automotive industry will transform IoT and provide IoT with a great boost. This technology has amazing potential and prospects.[10]

So after understanding the basic concepts we will be applying it here. So here we will be seeing as part of authentication part which is biometric systems which can be fingerprint and voice recognition. Now that will be seeing in the case of security part .Now after that for safety part a security issue will be taken and then it will be will analyzed and a solution or method will be provide which can produce a better result.

As we have seen previously the automobiles was mostly mechanical. Then As time went on we see the automobiles keep on evolving which introduced a lot of technologies like driverless technology and lot more."Float over text" should *not* be selected.

V. METHODOLOGIES

Inthisresearch,comparativeanalysiswillbecarriedoutbetwe enthedifferenttypes of biometrics used in authentication part of automobiles After analyzing a security policy will be taken and say what measures can be taken to improve it. A analysis will help understand which is the best biometric can be used. Comparison of these biometrics will take place based on 6parameters.

A. Voice Recognition

We see that voicing mainly uses distinct speech characteristics. It will highlight characteristics like voice pitch, speech style, voice tone, and voice frequency.

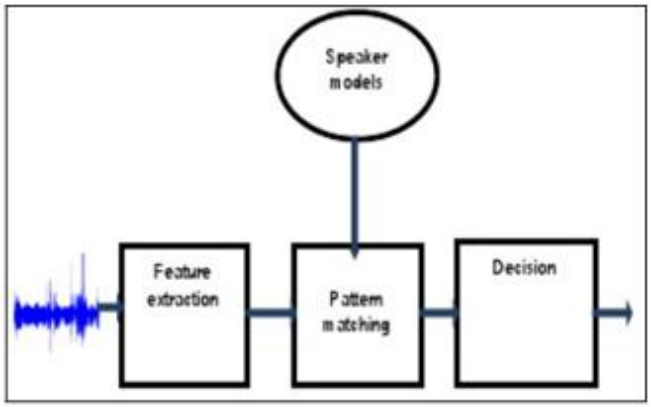

Figure 3:Voice Biometric Representation[10]

B. Fingerprint Recognition

For 2 purposes a Fingerprint scanner: -take pictures from the right user and scan the pattern of cranes and volleying.

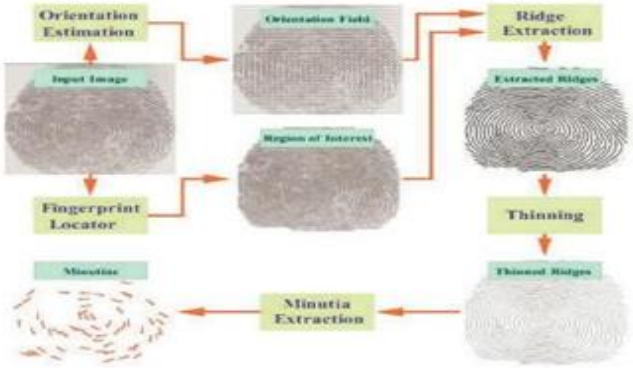

Figure 4: Schematic representation of fingerprintsystem[10]

We will then find that it is necessary, after programming into the SD card, in particular images of the ridges and valleys. The stores are encryptedin the form of binary code in every single fingerprint. The fingerprint or algorithm used can not be altered.

Table 1.6: Parameters Comparison Between Fingerprint and Voice

Biometric Methods	Fingerprint	Voice
Accuracy	Recognition Rate(85-95%) Match Rate < 2000 fingerprints per sec	Recognition Rate 70-90%
Dependency	FAR-0.0001% and FRR- <1%	FAR-0.01% and FRR-0.28%
Saftey	Encryption size-2500-4000bits	Encryption size-2000bits
User Friendly	Extraction Time<0.4 sec	Extraction Time -0.5 sec
Universality	Change in ligh exposure affects accuracy	Change in voice patterns
Money	Mid	Low

VI. ALGORITHM USED

A. Fingerprint Matching Technique

The most used fingerprint matching techniques are minutiae matching technique and pattern matching.

Minutiae MatchingTechnique

This is the technique that is mostly used by all like police and many people. Minutiae are rich characteristics found in every fingerprint. These Ridge characteristics are individual pieces that makes the general classes and subclasses. Identifying minutiae is what allows the fingerprint analysts to match prints to suspects. There are different types ofminutiae.

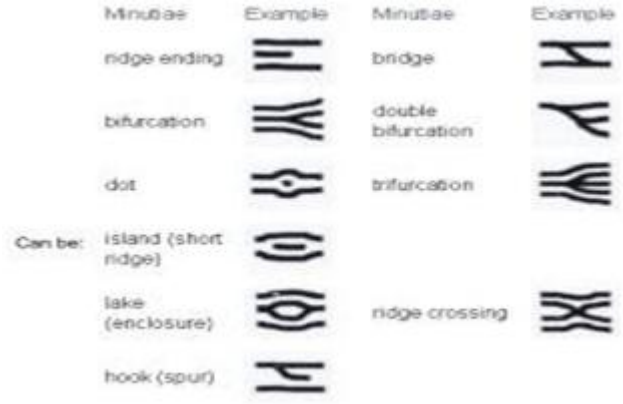

Figure 5:Different Minutiae[11]

Pattern Matching:

Pattern matching compares between two images and sees that which all images are similar. This is a technique that is used mostly to find duplicates.

Figure 6:Pattern Matching [12]

B. Voice Matching Algorithm

There are many voice matching algorithms such as Hidden Markov model(HMM),Gaussian Mixture model(GMM),Vector Quantization(VQ)

Hidden MarkovModel(HMM)

A hidden Markov model(HMM) has an emission sequence, but does not know the sequenceofstatesthroughwhichthemodelhasproducedemissions.AnalysesforMarkov hiddenmodelsseektorecoverfromtheobserveddatathesequenceofstates.Consider,for example, a Markov model with two states and six emissions. The model employs:

a)A red die, having six sides, labeled 1 through 6.

Let's consider a simple isolated word recognizer. The goal of such a system would find the most probable sequence of phonemes* given asequence of speech signal segments. Observationsinthedomainofspeechrecognitionarethesegmentsofspokenspeechsignal. Hidden states are the sequence of phonemes that we are looking to recognize. A phoneme based HMM for say the word 'cat' would have /k/ /a/ and /t/ as states. In this approach, we will need to create a HMM for every word in the corpus and train it to with the utterances of the word to strengthen the model. During recognition,these HMMs provideusanestimate(viaprobabilityscore)ifgivensequenceofspeechsegmentsmatches a string of phonemes. Since a string of phonemes can be mapped to a word,HMMs can used to find the most probable word for speech signal. Thus, HMMs are a corecomponent of speech recognition. Needless to say, the accuracy of recognition depends heavily on how effectively the HMMs have been trained. *A phoneme-based word HMM model will not scale for recognizing continuous speech since we will need to create a HMM forevery word in the corpus. For good recognition of continuous speech, you would need to use contextual triphone based sub-word HMMs.[13][14]

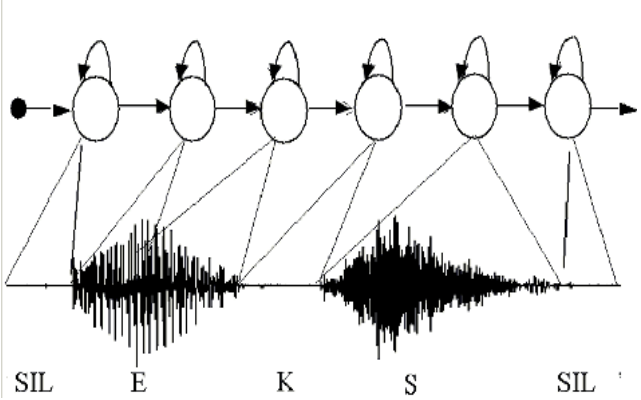

Figure 7:Hidden Markov model

Gaussian Mixture Model(GMM)

MM are basically used to model the speech feature distribution. It is not necessary to use only GMM to model this distribution, you could use DNNs also. So basically you extract features are for all the speech files(assuming you have 13 dimensional features) you can now go to this 13 dimension and see how the features are clustered.

They will have some pattern like all the speech features for a particular phoneme will be in one nice cluster and soon.Nowyourjobistolearnsomethingoutofthisdata.Youcould dokmeansclustering butpeoplealwaysgobyprobabilitymeasures,thatwayeasybecausewecanusemaximum likelihoodcriterionconcept.SoGMMbasicallygoesfitsthedata usingEMalgorithm.That waywareincreasingthelikelihoodofthedata.NowonceyoulearnGMMforeverystate ineveryphonemewecannowaskwhatistheprobabilitythatafeaturefromsomeutterance belongs to once of these states in one of these phones. We get a probabilistic answer from that. We feed this observation probability along with HMMs parameters to trace viterbi path for optimal word sequence.[15][16]

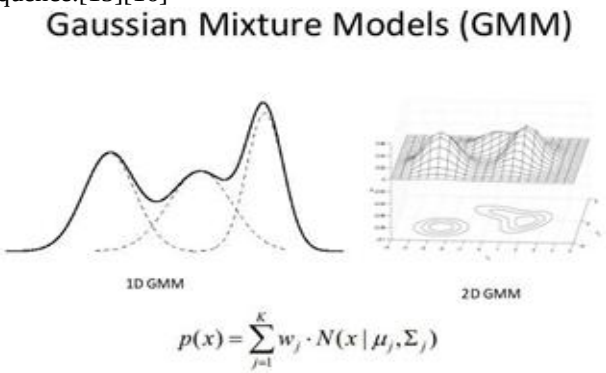

Figure 8:Gaussian Mixture model

Vector Quantization

The process which recognizes the speaker based onthe information present in the speech iscalledVoicerecognition.Thiscanbeusedtomanyapplicationslikeidentification, voice dialing, tele-shopping, voice based access services, information services, tele-banking, security control of confidential information. The variation of Speaker exists in speech signalsbecauseofdifferentresonancesofthevocaltract.MFCCisthetechniquetoexploit the differences of the speech signal. Similarly, the technique of Vector Quantization (VQ) emerged as useful tool. In this chapter, the VQ is employed for efficient creating the extractedfeaturevector.Theacousticvectorsextractedfrominputspeechofaspeakerand provide a set of training vectors. LBG algorithm is used for clustering a set of L training vectorsintoasetof Mcodebook vector. [15][16]

Figure 9:Vector Quantization.

C. Extra Algorithm

General bootstrappingarchitecture

General Bootstrapping Architecture (GBA), it is possible to provide seamless authenticationfor VoLTE Supplementary Services. GBA is standardized at the 3GPP. The user authentication is instantiated by a shared secret, one in the smartcard, for example a SIM card inside the mobile phone and the other is on the HLR/HSS. GBA authenticates by making a network component challenge the smartcard and verify that the answer is the one predicted by the HLR/HSS. Instead of asking the service provider to trust the BSF and relying on itfor every authentication request, the BSF establishes a shared secret between the sim card and the service provider. This shared secret is limited in time and for a specific domain.[15]

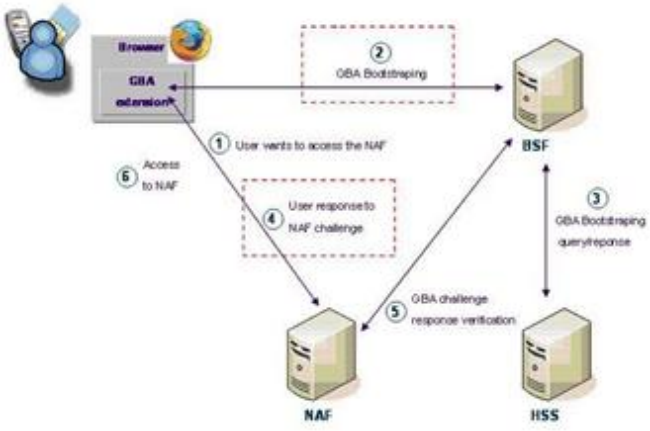

Figure 10:General BootstrappingArchitecture[16]

VII. MODULES USED IN FINGERPRINT SYSTEM

Intel Galileo gen 2 board

It is based on the Intel Quark 32-bit SOC. It is compatible with the Arduino Development Environment (SDE). It is compatible with Arduino software. It is single core 32 nm X1000 SOC with frequency of 400 MHz.

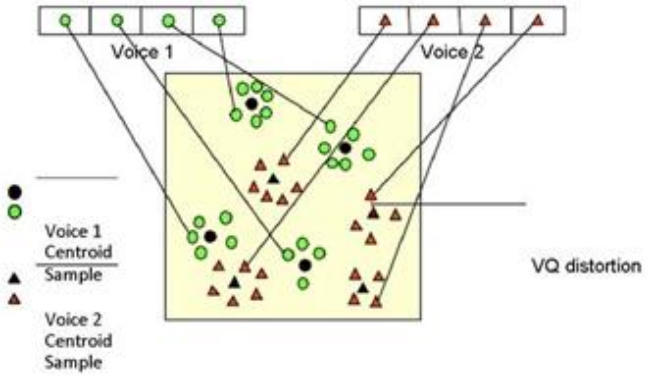

Figure 11:Intel Galileo gen 2 board GPS

GPSmoduleforIntelGalileoallowstoconnectyourintelboardtogetpositionandaltitudeaswell asspeed,dateandtimeonUTC.Itisperfectcomplementfordevelopingglocalizationapplications.

Figure 12:GPS Module

GSM:

It is basically a GSM Modem connected to PCB with different types of output taken from the board – say TTL Output and RS232 directly with a PC.

Figure 13:GSM Module

Wi-Fi Module

It is self-contained SOC with integrated TCP/Ip protocol stack that can give any microcontroller access to your Wi-Fi network. Its high degree of on-chip integration allows for minimal external circuitry, including the front-end module is designed to occupy minimal PCB area.

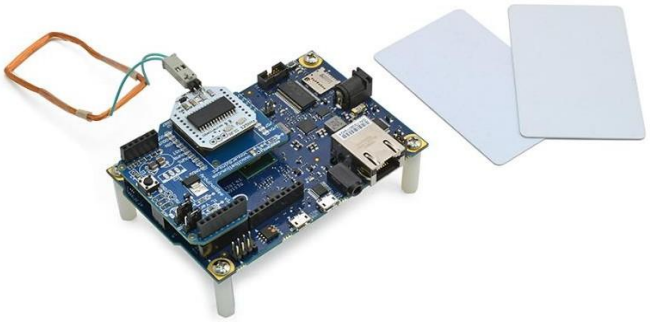

Figure 14:Wi-fi Module

SD Card

Micro SD cards are the smallest size of the cards. These cards are mostly used in many other devices such as tablets.it weighs just 0.25 gm.

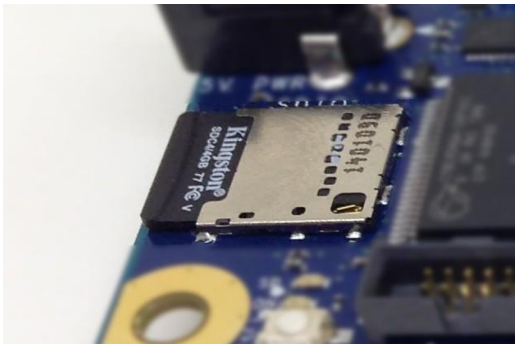

Figure 15:SD Card

VIII. MODULES USED IN VOICE RECOGNITION SYSTEM

U-BloxNEO-6Q GPS

TheNEO-6moduleseriesisafamilyofstand-aloneGPSreceivers featuringthehighperformance u-blox 6 positioning engine. These flexible and cost effective receivers offer numerous connectivity options in a miniature 16 x 12.2 x 2.4 mm package. Their compact architecture and power and memory options make NEO-6 modules ideal for battery operated mobile devices with very strict cost and spaceconstraints

Figure 16: u-blox NEO-6Q GPS MODULE

u-blox LEON g100 GSMModule

LEON-G1 series modules are cost efficient solutions offering full quad-band GSM / GPRS data and voice functionality in a compact LCC (Leadless Chip Carrier) form factor. Featuring low power consumption and GSM/GPRS class 10 data transmission with voice capability, LEON-G1 series modules combine baseband, RF transceiver, power management unit, and power amplifier in a single, easy-to-integrate solution

Figure 17:u-blox LEON G100 GSM Module

Arduino Uno microcontroller

ArduinoUnoisamicrocontrollerboardbasedonATmega328.Ith asa20digitalinput/outputpins of which can be used as a PWM outputs and 6 can be used at 16MHzresonator

Figure 18: Arduino Uno

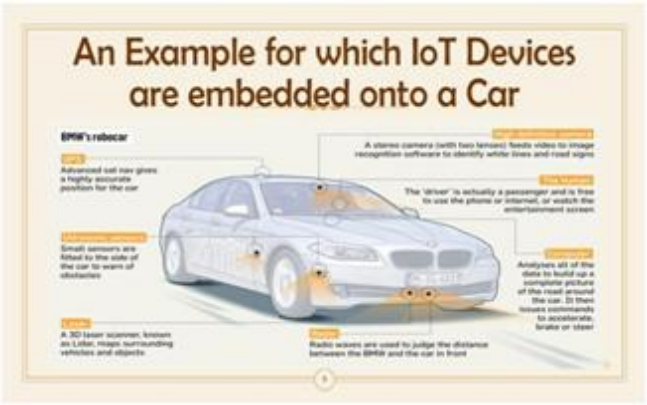

Figure 19: Sensors Are Embedded

IX. IMPLEMENTATION

We take a sensor example that is used in cars. In the field of IoT, there are security concerns in the car sector. Thus, there are some problems in it

- Endpoint impersonation
- Side- channel attacks
- Detection of endpoints compromised
- Ensure security at the risk of safety

Sensors in critical scenarios require extremely rapid working times, so asymmetrical encryption is not always feasible. So what a security model should be done in good time for critical time scenarios. Now take two cars, which approach each other with a known rate and security applications can prepare session clones for both cars before they reach a distance. before they reach a distance. If a critical scenario can not be detected if there is no time to renegotiate a safe session, secure communication between vehicles and sensors is guaranteed. That's why we can crash our car. For the precise answer, it is necessary to increase the implementation of the TCB. One alternative is GBA, which uses the UICC unit, which can distribute keys securely in the designed end points of the system. GBAs are the most suitable solution (Universal integrated circuit card). Even rudimentary endpoints, securing session keys for several critical scenarios, can be used in this protocol. Although heavy endpoints in public mathematics can not be critical, their benefit is that the environment can always be seeded from the root of confidence.[16]

X. ANALYSIS

Therefore, GBA can be used to distribute keys up to all endpoints of the system and does so in the boot-ups that ensure that old keys are not reused. After implementation of the solution, the vehicles sensor network will be well guarded. Whatever the changes we make, safety is the key. The car manufacturers must assess critical security technology and determine the weather, without jeopardizing their safety. The manufactures should ensure that whatever safety is important or implemented, it is the number one concern. [16]

XI. CONCLUSION

This paper is mainly focus on enforcing security features on the automobiles since usage of IoT,5G are being introduced. So By using the analysis that is generated from this paper firstwhatistobedoneisfirstwehavetointroduceasecurityassess ment.Despitethemedia hype, IoT solutions can be secured. Cost-effective security starts at the architectural level. Small changes can ensure the entire IoT product or service ecosystem is safe from abuse. But, in order to achieve this, the engineering team must take the time to build in security fromthegroundup:SecurityinIoTsolutionscannotbeimplement edasanadd-on.Itmust be a foundation. Now automobile manufactures are implementing security feature that is biometrics like Nisan.

REFERENCES

1. Code Institute, “What is IoT? Internet of Things - Code Institute Blog.” [Online]. Available: https://codeinstitute.net/blog/what-is-iot/.
2. V. K. Sehgal, S. Mehrotra, and H. Marwah, “Car security using Internet of Things,” 1st IEEE Int. Conf. Power Electron. Intell. Control Energy Syst. ICPEICES 2016, pp. 1–5, 2017
3. data varsity, “A Brief History of the Internet of Things - DATAVERSITY.” [Online]. Available: https://www.dataversity.net/brief-history-internet-things/#.
4. Actualitix, “Motor vehicle theft (rate per 100,000 population) by country - 2015.” [Online].
5. Available:https://en.actualitix.com/country/wld/motor-vehicle-theft.php
6. Shaon Shahnewaz, “Biometric Technology in Cars: An Introduction to the Future - M2SYS Blog On Biometric Technology,” m2sys. [Online]. Available:http://www.m2sys.com/blog/guest-blog-posts/biometric-in-car-future-technology/.
7. S. Sadhukhan, A. Acharyya, and R. Prasad, “Car Security System using Fingerprint Scanner and IOT,” vol. 10, no. October, pp. 1–4,2017
8. H. Nizam, M. Shah, M. Zamzuri, A. Rashid, and M. F. Abdollah, “Biometric_Voice_Recognition_In_Security_System_-_24_Pages.pdf, ” Indian J. Sci. Technol. Vol 7(2), 104–112, Febr. 2014, vol. ISSN (Prin, no. August,2017
9. N. Kiruthiga, L. Latha, and S. Thangasamy, “Real time biometrics based vehicle security system with GPS and GSM technology,” Procedia Comput. Sci., vol. 47, no. C, pp. 471–479,2014
10. U. R. J, “Remote Vehicle Tracking System through Voice Recognition App Using Smart Phone,” vol. 5, no. 6, pp. 200–205,2015
11. V. Vijigiri, V. Praneeth, M. Bhargava, and R. Chanduri, “Comparison of Iris, Finger, Voice Recognition Techniques-A Biometric Perspective,” 2017
12. being woven, “Even to the Minutiae | Being Woven.” [Online]. Available: https://beingwoven.org/2017/09/24/even-to-the-minutiae/.

13. Packt, “Implement Fingerprint detection technique using OpenCV 3 | Packt Hub,” 2015. [Online]. Available: https://hub.packtpub.com/fingerprint-detection-using- opencv/.
14. “Applying HMMs.” [Online]. Available: http://web.science.mq.edu.au/~cassidy/comp449/html/ch12s02.html.
15. Lawrence R. Rabiner, “A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition,”1989
16. wiki, “Generic Bootstrapping Architecture - Wikipedia.” [Online]. Available: https://en.wikipedia.org/wiki/Generic_Bootstrapping_Architecture
17. “Automotive IoT Security Countering the most common forms of attack.”

AUTHORS PROFILE

Shamik Palit is working as Assistant Professor in School of Engineering & Information Technology, Manipal Academy of Higher Education Dubai Campus. He is B.E. and M..Tech in Computer Science and Engineering ,currently pursuing PhD in the field of Computer Science . He has 16 years of teaching and industry experience.His field of interest is Software Systems Engineering , E Commerce, Enterprise Resource Planning. He has wide experience in design , development of enterprise applications.

Chandrima Sinha Roy is currently working as Assistant Professor in the field of Computer Science and Information Technologyin Eminent Institute of Management and Technology Kolkata. She is B.Tech. and M.Tech in Computer Science and Engineering. She has 8 years of teaching and industry experience. Her field of interest is Data Science and Web Technology. She has guided several engineering projects for undergraduate students.