

## A High Secured Ecc Based Iot Audiometric System For Cloud Based Dynamic Sensor Domain Environment

N.Bhaskar<sup>1</sup>, M.V. Ramanamurthy<sup>2</sup>, K. Jaya Sankar<sup>3</sup>, CRK Reddy<sup>4</sup>, Satyam Pulkam<sup>5</sup>

<sup>1</sup>Lecturer, Dept. of CS, Bhavan's Vivekananda College, Sainikpuri, Secunderabad, India

<sup>2</sup>Prof. & Head, Dept. of M&H, MGIT, Hyderabad, India

<sup>3</sup>Principal, MGIT, Hyderabad, India

<sup>4</sup>Prof. & Head, Dept. of CSE, MGIT, Hyderabad, India

<sup>5</sup>Department of Mathematics and Computer Science, Osmania University, Hyderabad

**Article History:** Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

### Abstract:

This paper is made based on the requirement of different domain users for effective hearing system. The system uses different devices to enhance the audio capability of different users at different application environment. The system uses IoT devices, sensors and different gateways for effective use of IoT based systems. The system will enhance the hearing capability of all users at different conference or personal or professional environments for the effective hearing capability among different hearing capabilities. It provides the environment to increase or decrease the volume of the source system based on the hearing capability of participants in the hearing environment. It can be used in any domain like conferences, home environment, education institutions and at public locations. It also adopts a security algorithm to protect the customer's data in encrypted format at cloud system. It recognizes the candidate at any time based on the ID assigned to an individual.

**Key Terms :** ECC (Elliptic Curve Cryptography), IoT (Internet of Things), Automated Audiometry, ICT (information and communication technologies).

### I Introduction

Hearing loss comes with age but can it may come to many people in life. According to the study, at least 25 out of 50 experience hearing loss. The process in which we can test the hearing loss is through audiometry.

An audiometry test will clear the hearing capability of a person. It tests the hearing intensity and tone of sounds. It also performs the hearing capability of inner ear. The audiologist can admin the hearing loss test and can advise the type of hearing aid to be used for the hearing problem.

The Fig.1 gives the graphical or digital response of hearing capacity of a person. It compares the standard capacity of hearing and a person's actual hearing capability to advise the hearing aid.

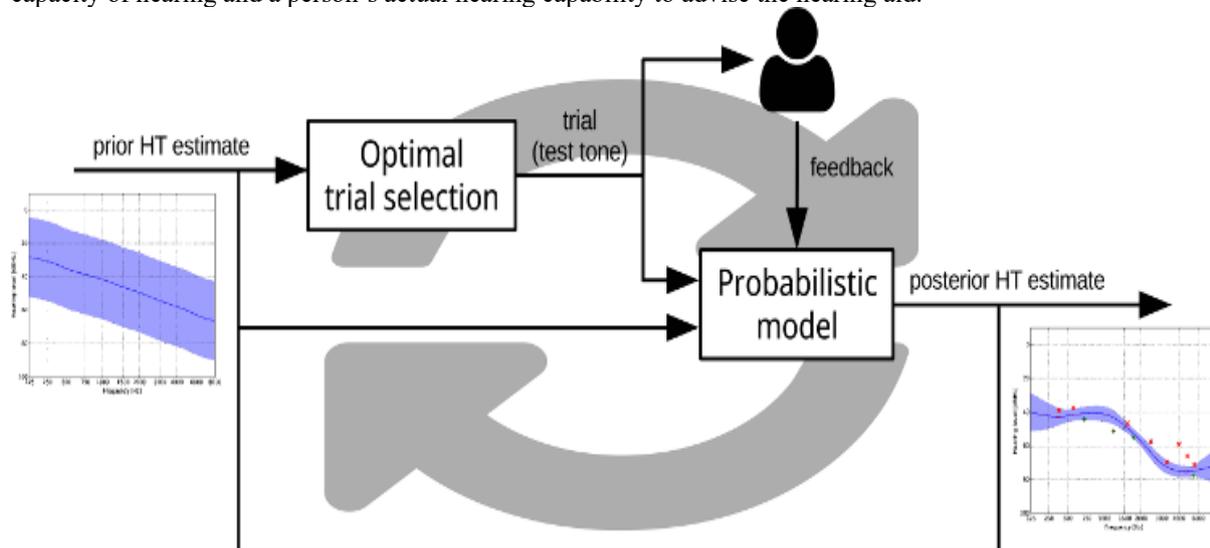


Fig 1 : Audiometry Process

### 1.1 IoT based hearing aids

The hearing loss or speech loss is affected by 5% of world population. The Fig.2 explains the procedure involved in providing hearing aids through sensors. Some people may hesitate to wear hearing aids. This paper presents the smart hearing aids to help the people suffering from hearing or speech problems. The hardware required to provide IoT based hearing aid consists of: hearing aid unit, Bluetooth based audio sensor, a program that provides application program interfaces(APIs) installed with programming. The mechanism used to communicate is text-to-speech and speech-to-text converters. The suggesting hearing aid should perform several tests like EMT related problems. It also tests the different degrees of hearing loss, the proposed devices help in assisting the patients suffering from hearing loss or speech loss.

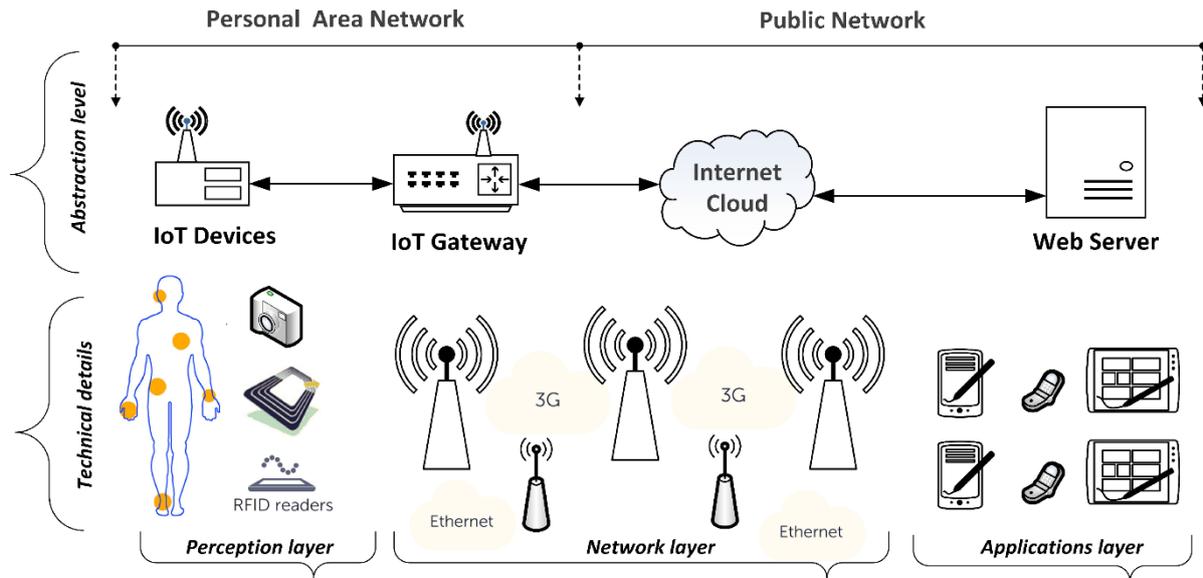


Fig 2 IoT based communication System

**1.2 Technical discussion about IoT and manual audiometry process**

The technical aspects involved in implementation of IoT based audiometry presented in Fig.3. The different components required are:

- Security
- Cloud based storage
- Network related issues
- Protocol suitable to implement

The hearing loss can may occur with different factors at different ages of a person. It is an “invisible” impairment, i.e. there wouldn’t be any external signs of the ear damage happened. It may happen gradually and insidiously over time. If a person ignores it, it may reach to an irreparable damage.

The digitization of many organization activities or products or services is going on. The domains like digital audiometers that incorporate ICT is a reality in the current market. The test performance of audiometric hearing evaluate a person’s hearing capability. It is possible to get results only with personal interaction. The market available hearing aids are manual tested devices. It is a part of medical information of a patient. The cost of such devices is high and need the research in cost reduction with more features. The Fig. 3 represents the interconnection among the components of the ECC encryption environment. The ECC is an efficient encryption for IoT based audiometric application environment. It is efficient because, the patient data must be safely stored, updated and retrieved for the purpose of successful implementation.

The purpose of ECC is to represent plane curve for a finite value to satisfy the curve equation  $y^2=x^3 + ax + b$ . Any point at curve can be mirrored on x-axis and curve will continue the same. Fig. 4 depicts a curve line to represent the communication process. Comparatively the ECC implementation gives more secured and has light weight data carrying algorithm when compared with the standard encryption algorithm RSA [1], [3], [7]. The ECC is preferred in IoT application environment due to low bandwidth utilization and component specific too.

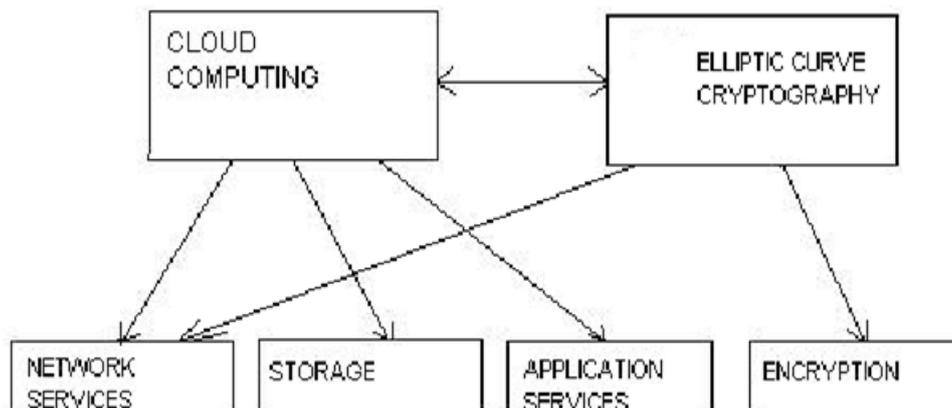
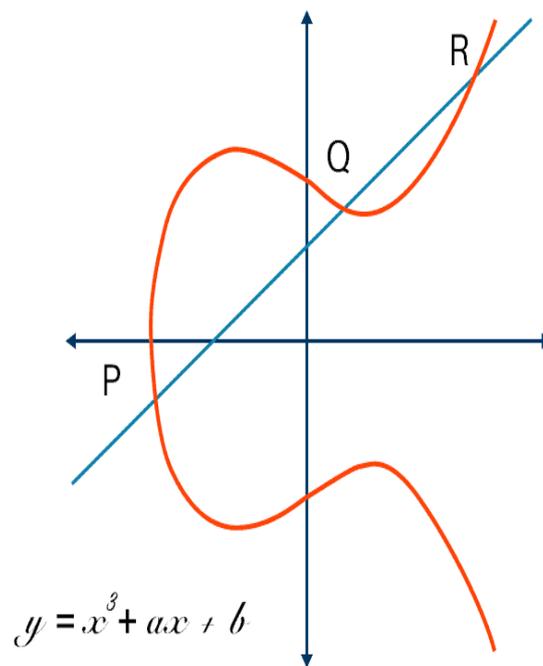


Fig. 3 : ECC in IoT based application environment.



**Fig. 4 : Example Elliptic Curve Crypto graph**

The Table-1 shows a sample survey of bandwidth utilization based on different domain participants for reference. It is the conclusion that we can use IoT based applications in health care environment because of low dropout of packets. It may consume more bandwidth, but it is advised because of packets dropouts are zero with sample data organized. The conversion process of audiometric encryption of voice received from the device to cloud and decryption of cloud stored data into devices.

Services	No. of users	Packet Drops (%)	Bandwidth Utilized (Mbps)
Health care	100	0	0.292968750
Banking	100	3	0.284179688
Transportation	100	5	0.205078125
Restaurant	100	7	0.146484375
Corporate	100	9	0.958007813

**Table 1 : Priority based response time for various domain requests.**

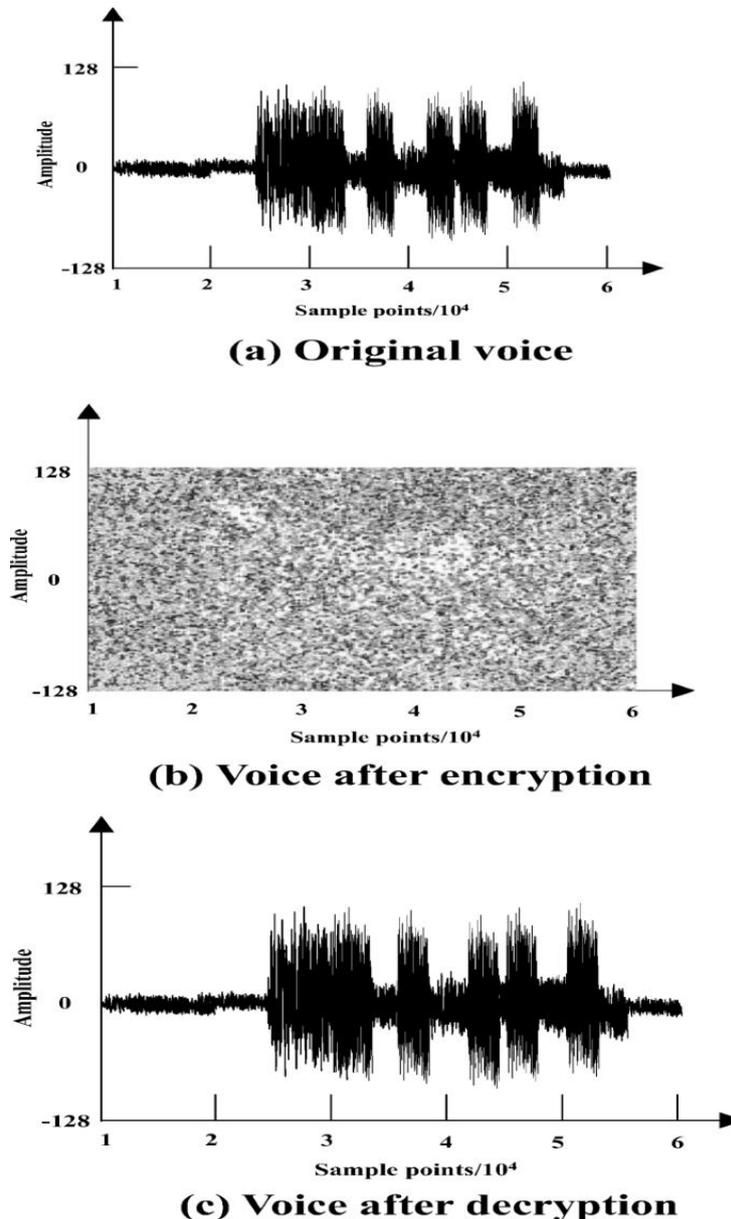


Fig. 5 : Voice encryption and decryption process in IoT based cloud environment.

## II Literature Survey

The different papers written on audiometry, IoT based data store and Security issues are discussed. The content are very interesting and helped to update research work.

1. The Automated Audiometry [10] is provided with the objective is required when there is no direct access. It helps to use hearing services and their services efficiently. It was not observed that there is no difference in accuracy of traditional and automated audiometry. The automated audiometry reduces the cost and increased accessibility.
2. The security for automated audiometry is performed efficiently with ECC [1]. The security is the challenge in many of the applications. Especially in cloud based audiometry storage require more security to prevent the privacy of the clients. The ECC is using a public key cryptography commonly used in cryptosystems. In the paper the author mentioned that the audio file is transmitted to the cloud in a secured manner as well as decrypting at the received end safely.
3. The paper [3] also discussed in detail about ECC implementation in IoT based applications. The ECC security is applied on moving vehicles in traffic to the traffic control room to prevent the accidents, safety alarms and area security. The secured mechanism available with ECC for key agreement and satellite to transmit the messages over vehicles. It also consumes a moderate speed of encryption during moving of objects.
4. The paper [7] providing the comparison between the traditional security algorithm RSA and IoT based applications supporting ECC. The traditional RSA applied on asymmetric cryptography algorithms which need the additional storage space for secret keys. It also requires huge encrypting key

length. The ECC provides the transmission of contactless biometric system. It provides more security with less key length and it does not require the passing of private key along with encrypted data. It also focuses on creating and sharing secret keys without transmitting private keys so that no one can access the secret key except themselves.

- In paper [8] the author discussed about traditional vs ECC security in IoT based systems. In one of the papers of Cisco mentioned that the ECC is the next generation crypto algorithm. It operates elliptic curve on finite fields. It is proved that the ECC is significantly better than traditional public key cryptography. Especially it can support the efficient security on IoT based applications.

### III Research related work done

**3.1 Proposed Architecture for IoT based Audiometry:** The proposed model consists of few layers to communicate between different components of architecture. The fig. 6 represents the elliptic curve to represent the layers proposed for successful communication with cloud internet. The layers participating to perform IoT based audiometry are:

**Physical Layer**

**Technical/Protocol Layer**

**IoT Layer**

**Application Layer**

**Layer**

**Physical Layer :** It consists of data stored at remote location to access and update about clients at cloud based database. Whenever a client connects to a remote cloud server and adjusts the sound accordingly.

**IoT Layer:** It provides the facility to use different protocols to communicate with cloud data server to exchange the data between the layers. They are like CoAP, MQTT, AMQP, DDS, ECC.

**Application Layer:** It gives great support to interact with system through some interfaces to access/update/create new client data. The applications that can be connected through mobile devices, IoT applications, Bluetooth applications etc.

**View Layer:** The user can connect to different layers through different devices for communication. The user can use any type of device through which they can communicate to the system.

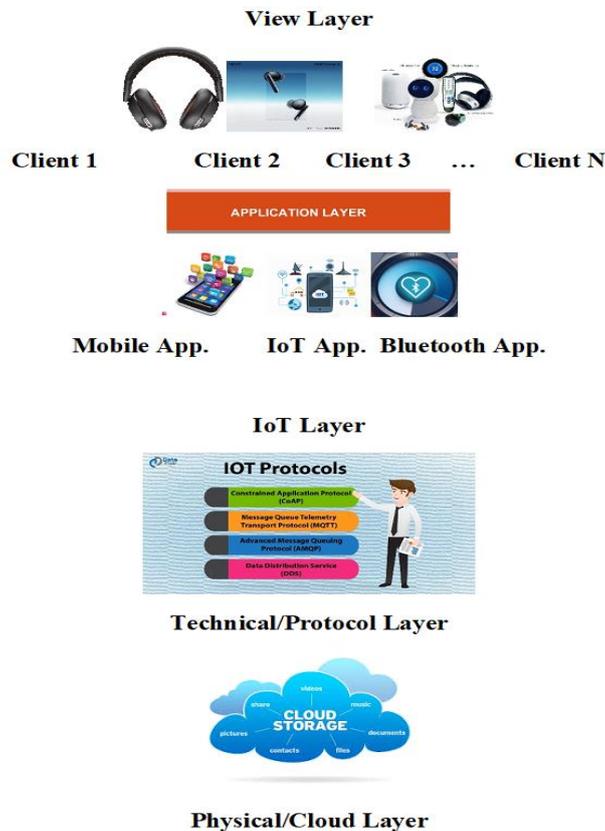


Fig. 6 : Proposed IoT based Audiometry architecture layers

**3.2 Algorithm :** An efficient algorithm is identified for successful implementation of ECC in the environment of IoT based applications. The following algorithm is advised to use in the specific IoT based audiometric sensing and successful implementation environment.

**Algorithm: Automated Sensor locating the candidate hearing details from cloud using previously stored User-id, DoU (Date of Update) and audio range.**

Step 1: Sense the candidate for existing or new user. Based on the user-id the details are detected.

Step 2: Verify left and right ears with any disturbance and without disturbance, then apply the automated audiometric for new updates or extracting the existing details when no change observed.

Step 3: Sense the audio frequency from the input source and decide the loss type sensor neural hearing loss, conductive hearing loss and mixed hearing loss [4][8]. The entire process of the following instances are performed using ECC which is identified as an efficient secured algorithm in IoT environment:

- Creating new client data in cloud for the first time.
- Updating the client existing stored values with the present scenario based data.
- Sensing the input frequency and hearing capability of the client and frequency modification accordingly.

Step 4: Increase or decrease the volume according to the input and hearing capability frequency.

Step 5: Repeat the Step 4 until the instrument disconnect from the user.

#### IV Conclusion and future work

It is concluded that the research work done on IoT based audiometric is very useful in different conferences, meetings with high success rate. The future work involved in this research work is to reduce the device size more compatible to different types of users and frequent updates in cloud storage according to the customer details identified. It is also suggested to communicate the users about the suggestions for audiometric improvement. The future work need to be taken for more security in transmitting the user data between devices and cloud and cost reduction of price in the implementation of devices for future reference.

#### References

1. "USING ELLIPTIC CURVE ENCRYPTION AND DECRYPTION FOR SECURING AUDIO MESSAGES", ArtanLuma ,BesnikSelimi , and LirimAmeti, · October 2015, DOI: 10.1007/978-94-017-9804-4\_42.
2. "Automated Audiometry: A Review of the Implementation and Evaluation Methods", Hassan Shojaemend, HalehAyatollahi, Review Article, Healthc Inform Res. 2018 October;,eISSN 2093-369X.
3. "ECC Based Lightweight Secure Message Conveyance Protocol for Satellite Communication in Internet of Vehicles (IoV)", Springer LinkC. T. Poomagal ,G. A. Sathish Kumar, 06 May 2020, DOIhttps://doi.org/10.1007/s11277-020-07285-3.
4. "A Secure and Efficient ECC-Based Scheme for Edge Computing and Internet of Things", Hisham AlMajed, Ahmad AlMogren, 29 October 2020, Sensors 2020, 20, 6158; doi:10.3390/s20216158.
5. "Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing", T Daisy Premila Bai, S Albert Rabara, A Vimal Jerald, IJCST Vol. 6, Issue 3, July - Sept 2015, ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print).
6. "Network Security Using ECC with Biometric", Dindayal Mahto and Dilip Kumar Yadav ,May 2001, IEEE Symposium on Security and Privacy.
7. "A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices", Manuel Suárez-Albela , Paula Fraga-Lamas, Tiago M. Fernández-Caramés, 10 November 2018, sensors, doi:10.3390/s18113868, www.mdpi.com/journal/sensors.
8. "Signal Processing for Cryptography and Security Applications", Miroslav Knežević, July 2010, In book: Handbook of Signal Processing Systems (pp.161-177), LejlaBatina,Junfeng Fan, Springer, 2006, The SHA-3 Zoo. [http://ehash.iaik.tugraz.at/wiki/The\\_SHA-3\\_Zoo](http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo).
9. "Evaluation of Apple iOS-based automated audiometry", Yuan Xing, Zhen Fu, Xihong Wu, Jing Chen, Buenos Aires – 5 to 9 September, 2016 Acoustics for the 21st Century.
10. "Automated Audiometry: A Review of the Implementation and Evaluation Methods", Hassan Shojaemend, Published online 2018 Oct 31. doi: 10.4258/hir.2018.24.4.263.