International Journal of Research in Engineering, Science and Management
Volume-2, Issue-3, March-2019
www.ijresm.com | ISSN (Online): 2581-5792

Multiple Scenario based Data Transfer using Ultrasound through Smart Phone

M. Rahul[1], N. Thamizhselvan[2], P. Priyadharshini[3], P. Veeralakshmi[4]

[1,2]Student, Dept. of Information Tech., Prince Shri Venkateshwara Padmavathy Engg. College, Chennai, India
[3]Asst. Prof., Dept. of Information Tech., Prince Shri Venkateshwara Padmavathy Engg. College, Chennai, India
[4]Assoc. Prof., Dept. of Info. Tech., Prince Shri Venkateshwara Padmavathy Engg. College, Chennai, India

***Abstract*: Internet of Things (IoT) has more number of options to communicate but in single place commanding we need smartphone technologies for interaction. Here we are using Ultrasound based communication. Some companies are using IoT for reducing the human works for reaching speed service to customers. Some companies are aiming people needs to reduced their work in a single place by using the smartphone. More people were using smartphone for communication in different ways but here we are using for device interaction with ultrasound technology as good. For communication in IoT environment, we use some URL concept for secure requesting system, we proposed the sound namely ultrasound, it uses normal speakers that was used in smartphone. It is very useful in secured communication over devices in IoT environment. Devices are expecting the fast command travel from the source but here it is very quick and high Directional. Also is secured in communication and may use in various area but we have used in ecommerce application for testing the accuracy.**

***Keywords*: Secured data, IoT, Application, Administration, user registration**

1. Introduction

Mobile Phone communication has more number of ways to share their data with each other, in recent times, which is very fast is very important. Some technologies are developed to exchange the data using the reference called phone number, more are the other is application, SMS oriented communication. Some technologies are used in base namely Bluetooth, Wi-Fi, near filed communication (NFC). There are more advantages in these technologies, very quick and flexible. Bluetooth is used to communicate by pairing the device with each other. This model has more security options and can apply later by the mobile phone companies. NFC is the option for communicating the data in a short range options. Wi-Fi is the scheme for connecting more devices with each other to communicate in a range. This types of technologies are used to protect the data communication with each other, our proposed system is used the sound system for communication in a secure way for long and shorter distance. Hence we have proved the accuracy level by comparing with existing system on time and speed. In existing system, there are more level of communication does not have security patches but in our system we have introduced the special scheme to secure the IoT platform and the data which is traveling in the environment. This ultra sound will travel in a fast to reach every device which was command. Later it will be analyzed for seeing the accuracy and speed. There some options we have introduced her namely one-time password (OTP), Registration, Creating Application for testing and tested the speech over application for increasing the response speed.

2. Related work

Some options were here to switch off or on the device or light by the command basis or by the URL basis but using this device may get confused later [1]. Testing the speech by choosing anyone of the technologies out of is very worst but using in relevant area, it was achieved [2], [3] Testing in real world scheme, we have used IoT level communication for speed up the data communication using smartphone relating the application and security terms and further [4], NFC is the technology used for transmitting the data without any pairing permission, it was created for the immediate transmission but here it was used in IoT devices for giving flexibilities to the people in the market. There are more number of advantages and dis advantages are discussed, using this system we have proposed the scheme in Ultra sound model for reducing the scheme. NFC is used to reduce the long range transfer problem and it has short range problem, comparing Bluetooth it does not have any security options [5], Bluetooth and other models like Wi-Fi is also has another types for displaying the scenarios. This options were considerable for the data communication and for device satisfaction. There is more area to satisfy the fast communication, but in our system we have proposed the accuracy concept for satisfying the speed of consumer type of network applications that is relating the router. Access point has some rules like allowing the particular system to the environment for access the system in a safe way. Moving from one place to other place is not a matter but in a secured and speed way is very important than the all. In our system we have achieved the speed and accuracy further. There are more number options are taking after the more survey was reached by the researchers. Here we have surveyed the system very well for comparison and satisfying the system to bring a good architect and good IoT based communication. Security problems in NFC, Bluetooth and Wi-Fi was displayed on comparison satisfactions [6], [7] and Recent concepts and area are discussed for implementing the IoT based Ultra sound communication in further [8]-[10].

3. Proposed system

This paper proposes the ultrasound based data communication with IoT platform for satisfying the system in heavy security and aped models. We are compared the modulation and demodulation scheme because this concept is not audible to the users in future so we have proposed the scheme in Ultrasound methods for satisfaction. We proposed the library for running the devices in low power schemes and for increasing the security to the high for satisfying the users for making this product good.

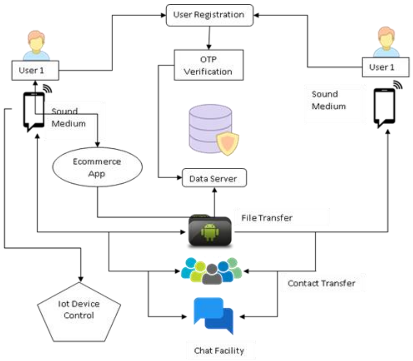

Fig. 1. System model

A. *User Registration & OTP Verification*

Before using the application user needs to register for security name they have to enter their name, email id and phone number for generating the one-time password (OTP). After registering, the application will send the message to the user's phone number like OTP number as like SMS, in that they will some unique number for entering in the web page for completing the registration, after registration, user will have permitted to access the page in secured way. Using this scheme, user will be safe to use any application for requesting their need in secured way.

B. *Ecommerce Web Application*

A software application for shopping, securing the cart, information of the user and so on. This scheme will act like security application, every information will be auditing before it gets to the user side. This scheme will have methods like a request as shown in Fig. 1 with permission or analyzing the person before accepting. Some hackers will install the virus filled an application to the computer or to the network connected server that system will act as a hacker for a long time without knowing us. In these cases, our proposed system will detect the fake application and removing it completely from the system.

C. *Sound generation & customization*

After the process, user can choose the mode of sound to communicate with each other using the application then they can customize the level of sound and then using in application is very customizable. There are some options to use the sound wave in a manner. We have used the concept for generating the simple steps. There more area was satisfied using this concept and achieved the accuracy level as good.

D. *Secured data transfer and IoT device control*

It is the concept which is used to secure the user from unauthorized access or unauthorized user. Malicious will return every time when a user online. On that time, we no need afraid of. This system of method will reduce and delete the malicious information from the hackers. There are more options were developed in this paper on comparing the previous paper. We have achieved the system development. Our survey will demonstrate everything about IoT security. User can also monitor the devices through the application and from the smartphone SMS scheme. We have used the proposed scheme for securing the communication over IoT using Ultra sound scheme.

4. Experimental results

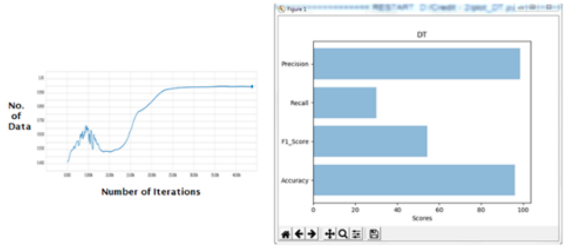

Fig. 2. Training data and Execution

In Fig. 2, the accuracy with that the projected system can classify the user data from the analysis set using ultrasound. Again, here you'll be able to observe that with the increasing variety of iterations in coaching, Associate in ever bigger level of accuracy is achieved. Upon completion of the coaching, the analysis set was given a final classification to determine the accuracy with that the projected system will classify the orders. The accuracy achieved on the coaching information – or the proportion of sound that the theme was ready to classify properly.

5. Conclusion

More usage is occurring in Smart phone related IoT environment as same to this, there is a number of problems are also occurring. To solve these issues and complexity, we have proposed the special software model for protecting the communication which is getting affected by a spammer in the IoT environment. The result was achieved by Ultrasound scheme with analyzing models. There some comparison shows up well and proposed as per the details proceeded by the researchers. In future work, this method can be used in any region for securing the user message and personal information.

References

[1] C. Pereira, A. Pinto, A. Aguiar, P. Rocha, F. Santiago, and J. Sousa, “IoT interoperability for actuating applications through standardized m2m communications,” in 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1– 6, June 2016.

[2] G. Elert, “Frequency range of human hearing,” September 2014.
http: //hypertextbook.com/facts/2003/ChrisDAmbrose.shtml.

[3] K. Ashihara, “Hearing thresholds for pure tones above 16khz,” The Journal of the Acoustical Society of America, vol. 122, no. 3, pp. EL52–EL57, 2007.

[4] V. N. P. Rajalakshmi Nandakumar, Krishna Kant Chintalapudi and R. Venkatesan, “Dhwani: Secure peer-to-peer acoustic nfc,” in Proceed- ings of ACM SIGCOMM 2013, Sigcomm ’13, (New York, NY, USA), ACM, 2013.

[5] “ECMA”, “Near field communication interface and protocol (nfcip-1),” June 2013. http://www.ecma-international.org/publications/standards/Ecma-340.htm.

[6] T. Baker, “Up to what distance can near field communication (nfc) operate?,” May 2011.

[7] Wikipedia, “Wikipedia nfc article,” August 2013. http://en.wikipedia.org/wiki/Near field communication.

[8] J. J. Gummeson, B. Priyantha, D. Ganesan, D. Thrasher, and P. Zhang, “Engarde: Protecting the mobile phone from malicious nfc interactions,” in Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys ’13, (New York, NY, USA), pp. 445–458, ACM, 2013.

[9] R. Zhou and G. Xing, “nshield: A noninvasive nfc security system for mobiledevices,” in Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services, MobiSys ’14, (New York, NY, USA), pp. 95–108, ACM, 2014.

[10] V. Gerasimov and W. Bender, “Things that talk: using sound for device-to-device and device-to-human communication,” IBM Syst. J., vol. 39, pp. 530–546, July 2000.