Research Journal of Applied Sciences, Engineering and Technology 13(4): 325-330, 2016
DOI:10.19026/rjaset.13.2949
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: March 21, 2016 Accepted: May 5, 2016 Published: August 15, 2016

Research Article

Secured Seamless Broadcasting Using Bluetooth Enabled IoT Cloud

[1]B. Nagajayanthi, [2]V. Vijayakumari and [3]R. Radhakrishnan
[1]School of Electronics Engineering, VIT University, Chennai,
[2]Department of ECE, Sri Krishna College of Technology, Coimbatore,
[3]Department of ECE, Vidhya Mandhir Institute of Technology, Erode, India

Abstract: Bluetooth Smart 4.2 or Bluetooth Low Energy wireless protocol has made the Internet of Things (IoT) a reality with its low power, low cost and an added Internet Protocol Support Profile. The range of standard Bluetooth is limited but Bluetooth empowers developers and manufacturers to quickly create the next level IoT innovation. Location independence increases utility. It helps people to work virtually smarter from any place. IP Based mobile wearable devices, sensor nodes and applications allow people to stay connected irrespective of the location. Mobile apps connect the Bluetooth Enabled devices over Internet to exchange data thereby overcoming the distance limitation of Bluetooth and making the Bluetooth Enabled devices separated by larger distances to communicate. Data is obtained from sensor nodes and transferred to a Cloud by using a Mobile App. Data is retrieved from the Cloud by a remote Bluetooth Enabled device. As the innovations bloom there remains a security threat when data is stored in the cloud. Bluetooth addresses IoT security by authentication, association, encryption and privacy. Security measures need to be tightened to ensure the security of data. Authentication and Encryption is done by a unique pattern for secured transfer of data through a Bluetooth enabled Cloud. The proposed method bridges the gap between usability and security by increasing the range of transmission.

Keywords: Authentication, cloud and location independence, encryption, internet-of-things, range extension

INTRODUCTION

The IoT landscape grows in a rapid pace. Bluetooth Smart enables Internet Connectivity using IPv6. The Internet Protocol Support Profile (IPSP) enables seamless connectivity over IPv6, the backbone for the Internet of Things. IPv6 provides tools which are well designed for sensor nodes. IP Based Interoperability is inherent in Bluetooth so there is no requirement for an additional gateway. Figure 1 depicts IoT where Internet of things links the world of Bluetooth enabled devices wirelessly using RF wave sand allows the devices to communicate using the Internet by shaping the network of smart objects. Bluetooth operates in the unlicensed 2.4 GHz ISM band (Industrial, Scientific and Medicinal Band). Bluetooth is inherent in most of the devices used in our day to day life or it can be integrated into the devices through USB or parallel port. Bluetooth connects devices within a limited range virtually to exchange voice and data. Sharing the data with preserved privacy is the need for the digital world. The latest Bluetooth Smart focuses on stronger security, privacy, seamless connectivity over the Internet with high data rate, mesh networking, longer range and high speed. It heralds a new wave of Bluetooth products and accelerates growth in the emerging categories such as wearable, smart homes, healthcare and smart location tracking.

Fig. 1: Internet-of-Things (IoT)

Conventional Bluetooth operates in a personal area network within a limited range. In our current approach, Mobile Apps are integrated with Bluetooth Enabled Devices to transfer data over longer distances using Bluetooth Enabled IoT Cloud.

This range limitation is extended over longer distances by connecting Bluetooth Enabled devices over a Cloud. Security of the data is ensured by enhanced Authentication and Encryption. Authentication is ensured by exchanging a dynamically generated non-orthogonal pattern between the Master and the Slave for verification.

Corresponding Author: B. Nagajayanthi, School of Electronics Engineering, VIT University, Chennai, India

LITERATURE REVIEW

The existing range of operation in Bluetooth ranges from 1 m to 100 meter depending on the transmit power. Range can be extended by using specialized antennas. Table 1 summarizes the range of operation with varying transmit power. Throughput and data rate depends on the version of Bluetooth.

Preetha (2011) has proposed a routing technique to increase the range of transmission. Range can be increased by using routing techniques that update the neighboring devices information. The network uses intermediate nodes to increase the range of transmission.

Bluetooth uses Adaptive Frequency Hopping (AFH) and the devices hop over frequencies in random avoiding the occupied channels. Kumar *et al*. (2012) have extended the range in Bluetooth by soldering an external Omni-directional antenna which is 28.5 centimeter long to the Dongle. Vemuru (2011) has published a whitepaper which increased the throughput by using Beam forming technique.

Bluetooth smart support for IoT: Bluetooth Smart provides Support for IoT devices. Bluetooth is a short wave, cable free, ad-hoc, free to use low power personal area technology. Bluetooth is preferred because it is interoperable and operates on heterogeneous devices. Health risks are mitigated as the devices are operating at low power. Collotta and Pau (2015) substantiates the need for Bluetooth in healthcare and emerging applications due to its low power consumption and reduced interference. Interference between the devices is reduced by using Adaptive Frequency Hopping technique. Bluetooth does not require Line-of-Sight (LOS) and the data can be broadcast through walls. The symmetric configuration of Bluetooth where a slave in one piconet can act as a master in another piconet using Time Division Multiplexing paves way for more challenging innovative solutions.

Bluetooth Special Interest Group (SIG) (Kirkland, 2016) has announced in February 2016 that Bluetooth Low Energy (BLE) devices can be directly connected with the Internet using Bluetooth RESTful APIs and HTTP Proxy Services. But the problem is Bluetooth API needs a Gateway which will serve as a security threat for the data and HTTP Proxy service does not perform well on heterogeneous devices.

Bluetooth is preferred over Wi-Fi because based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol the contention-based approaches could not guarantee an upper bound on the medium access delay which makes it inappropriate for time-constrained traffic and for applications that necessitate low power consumption. The added functionality in Bluetooth Low Energy (BLE) to operate in the suspended state for extended periods of time is preferred over the other technologies as Bluetooth is inherent in almost all the devices used in our day to day life. The networking nature of the devices supports on-line streaming services to control the device functionality over the network.

Table 1: Operating range of blue tooth

Class	Maximum Power	Range
Class 1	100mW (20dBm)	100 m
Class 2	2.5mW (4dBm)	10 m
Class 3	1mW (0dBm)	1 m

Bluetooth is used for broadcasting any multimedia data not exceeding 500 KB size. Data can be transmitted without interference even in the presence of Wi-Fi Communication. Communication can occur between a Master and a Slave but not between Slaves. Devices communicate over longer distances by connecting itself to the Internet. Bluetooth Enabled devices can access information from a distant place.

ARCHITECTURE FOR SEAMLESS BROADCASTING USING BLUETOOTH ENABLED IoT CLOUD

Short range radio technologies are used to connect groups of small workforce devices to the Internet, via capillary gateways and cellular networks. Bluetooth enabled devices constitute the master and the slave. The one that initiates data transfer forms the Master and the remaining form the Slave. They are connected in an ad-hoc fashion to form the Piconet. Several such Piconets form the Scatternet. With the advent of Bluetooth Smart version 4.2 data can be exchanged between any BLE devices via the Internet through the mesh network.

IoT sensor nodes capture bio-medical and context signals from patient's body and communicate the sensed data to remote healthcare monitoring system through a Bluetooth Enabled IoT cloud for treatment and diagnosis as depicted in Fig. 2. Data is stored in the cloud for retrieval. A patient is monitored and his details are sent to the hospital for healthcare. The sensor nodes are deployed in the patient's body which measures the relevant parameters. Authentication is done at the IoT node and the details are transferred to the server at the hospital. When the sensitive data is transferred through the cloud data should be secured.

Nagajayanthi *et al*. (2015) has improved authentication by using a unique non-orthogonal pattern for authentication instead of the conventional key exchange. Security is defined at the application layer and at the link layer. A Multilayer Security Linear Programmable Pre-coded Matrix Decomposition Method (MS-LPMD) is used to generate a non-orthogonal dynamic pattern for authentication and Encryption between the sensor node and the Hospital

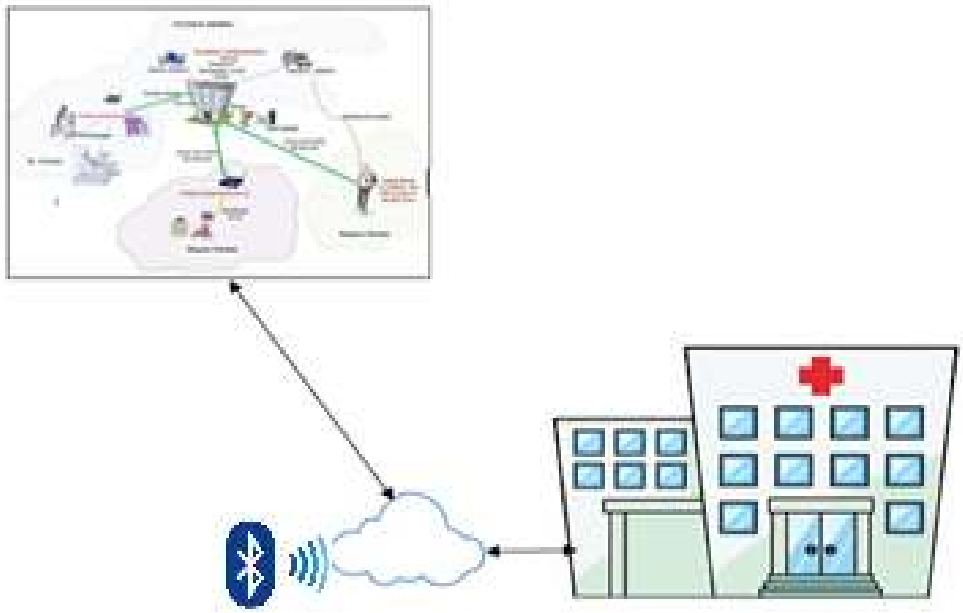

Fig. 2: IoT enabled transfer using bluetooth for healthcare

server. A non- orthogonal 64*64 matrix is generated and a small sized 64×1 matrix is randomly picked. This random unique matrix pattern is picked and sent to all IoT Nodes. The column coefficients are combined to form a unique pattern by the IoT node. From the generated pattern, a cipher key is generated which is used for encrypting the data. The generated cipher key is shared with the hospital server for decrypting the data. The data is transferred from the sensor node to the hospital server which is separated by a distance. It was not possible to reconstruct the data.

In Bluetooth Smart a dedicated data channel for IPv6 communications is added and the ground work has been laid for assigning IP addresses to Bluetooth devices. Chatziefthymiou and Goudos (2015) have envisioned future smart cities using IoT. Gubbi *et al*. (2013) have analyzed the perspectives involved in IoT.

The basic components of the proposed architecture for increasing the range of transmission between the sensor node and the hospital server include:

- Bluetooth Enabled Devices which include the sensor node and the hospital server forming an ad-hoc mesh network to exchange information.
- A Cloud acting as a Web Server to store and retrieve information from anywhere.
- Client receives the information. The sensor node captures the information and sends it to the server at the hospital.

Client communicates with the server using an Android App. A User Interface is developed using XML in the Client. XML is used for customizing using a GUI (Graphical User Interface). An Android App is created and a camera app is integrated along with the Android App using Eclipse in the mobile which serves as the Client. The sensor sends the information to the Android App. The Android App is linked with the Worldwide Web to send all the captured data to a software Cloud platform. Cloud stores huge amount of data for analysis. The Bluetooth enabled mobile captures and stores the image in the SD card. This path is given for the data to be transferred to the Cloud. Android Development Tool (ADT) is used for customizing the User Interface.

The Laptop serves as the Cloud using the WampServer. The Local Host displays all the images and files uploaded in the Cloud. Android Application Package (APK) is a package file format used by the Android operating system for distribution and installation of mobile apps and middleware. For the application developed, an APK is created and exported to the mobile.

The WAMP stack provides the modules needed for a Web server which includes an operating system, database, Web server and Web scripting software. WampServer used in Web Server environments provides a Windows friendly platform for Apache, MySQL and PHP based Apps. WampServer (Windows/Apache/MySQL/PHP, (and/or) PERL combined with Microsoft Windows) forms a stack and creates web applications with PHP and MySQL database. In this stack, Microsoft Windows serves as the Operating System (OS), Apache as the Web server, MySQL handles the database components, while PHP, Python and PERL serve as the scripting languages.

Tests related to the connectivity between the Cloud and the local server was done by checking with the IP Server.

Programming was done in Java to allow interoperability between the devices. Bluetooth devices enter into the inquiry state to discover other Bluetooth devices. Bluetooth devices in the broadcast range and in the discoverable mode will respond. So, with the use of all these technologies Bluetooth enabled systems can provide user friendly interface which provides multi-platform on which different operating systems like android, windows etc. can be incorporated. As the systems are platform independent users can use heterogeneous devices with different operating systems. User can utilize the application oriented apps by consorting through various authentication methods. Thorat *et al*. (2016) has suggested different methodologies to transfer using cloud. Data can be shared among two or more devices over cloud and data can be easily store and maintain with the help of cloud storage.

RESULTS

Cancerous cell image and sensor data was transferred with enhanced authentication and encryption in the presence of an attacker. A pattern was exchanged for authentication and a portion of the generated pattern was used for encrypting the data. Figure 3 pictorially represents a piconet with 4 nodes forming the slave and a master. The scenario was tested with the transfer of data in the presence of an attacker. Figure 4 shows the encrypted sensor data using MS-LPMD. Figure 5 shows the decrypted data. With

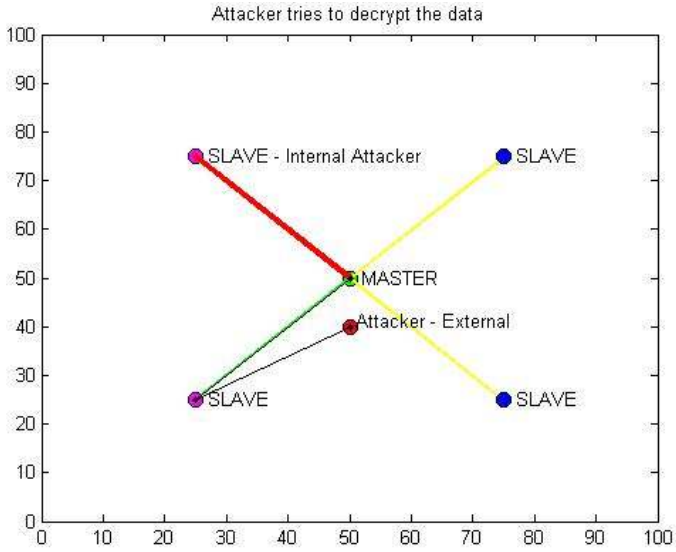

Fig. 3: Piconet with master, slave and attacker

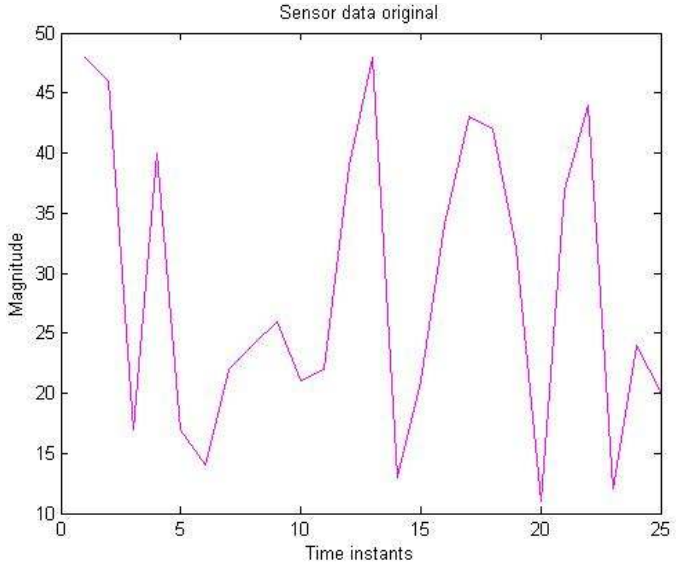

Fig. 4: Sensor data sent is encrypted

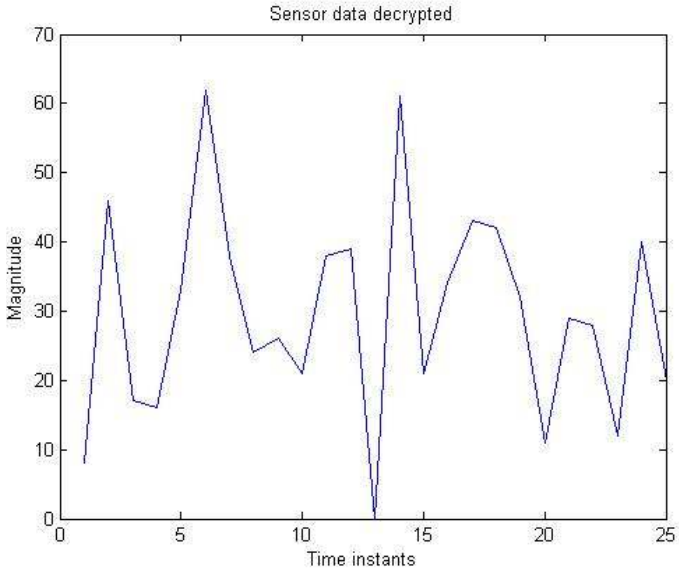

Fig. 5: Attacker is not able to decrypt the data

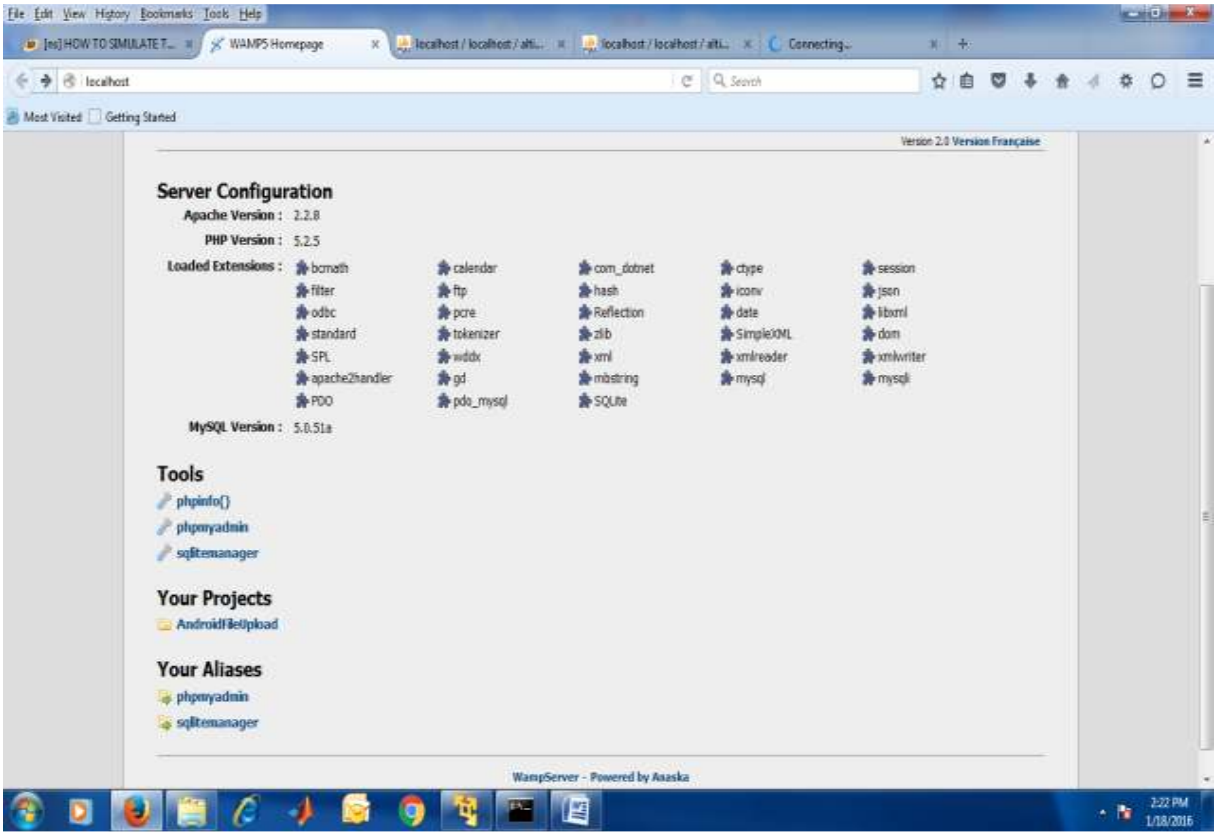

Fig. 6: PhpMyAdmin acts as the database

secured authentication using MS-LPMD the attacker failed to decrypt the data. Figure 6 shows the PhpMyAdmin which acts as the database. PhpMyAdmin manages the database which stores the information related to the details of the data stored. These details are stored in the cloud which acts as the server. From the cloud the data can be stored and retrieved. The test was performed with Bluetooth Enabled Mobile acting as the client and Laptop serving as a Cloud. Using the APK downloaded in the mobile for the application the Mobile captures the data (Fig. 7). The captured data is loaded onto the server (Fig. 8). On activating the App the devices become Bluetooth Enabled. The Wampserver converts the server into a

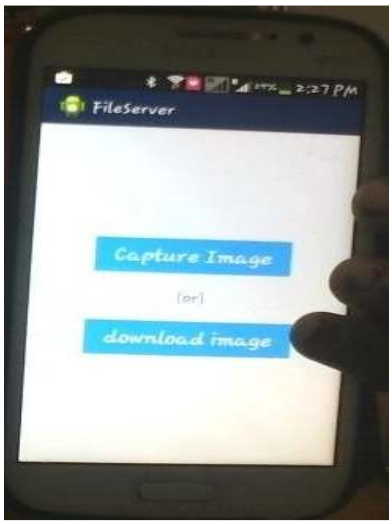

Fig. 7: Images are captured and stored by the Android App

Fig. 8: Images are loaded onto the server

cloud. The data is transferred from the Android App in a Bluetooth Enabled Mobile to the Bluetooth enabled IoT Cloud.

CONCLUSION

The major innovation involved in the development of a Bluetooth Enabled IoT Cloud for exchanging data between Bluetooth Enabled devices which are separated by a distance. The increase in range is four times more than a conventional personal area network range of up to 10 m. Bluetooth enabled devices can be deployed indoors or outdoors. Due to streamlined transfer increased speed was obtained. The speed in which data is transmitted in IoT deployments has introduced new possibilities for real-time services in healthcare but there are critical infrastructure requirements for security. Security is tightened using MS-LPMD approach. Yet another advantage is mesh networking, which is a key architecture for the IoT. Mesh is a network topology which allows devices to be interconnected between network nodes. Each node can accept and forward data to another node. This architecture provides economical scalability and easier deployment.ABI research forecasts that by 2018, there will be over 10 billion Bluetooth-enabled devices in the marketplace. Bluetooth Smart forms a vital part in IoT by providing power efficient and cost effective solutions. By increasing the range of Bluetooth, Bluetooth Smart is going beyond enabling the internet of my things and makes the 'internet of everything' a reality. Bluetooth lacks user authentication which can be implemented by combining device authentication along with user authentication.

REFERENCES

Chatziefthymiou, S. and S.K. Goudos, 2015. A survey of IoT: Architecture, applications and future vision. Proceeding of the 4th International Conference on Modern Circuits and Systems Technologies. pp: 1-3.

Collotta, M. and G. Pau, 2015. Bluetooth for internet of things: A fuzzy approach to improve power management in smart homes. Comput. Electr. Eng., 44: 137-152.

Gubbi, J., R. Buyya, S. Marusic and M. Palaniswami, 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Gener. Comp. Sy., 29(7): 1645-1660.

Kirkland, W.A., 2016. Bluetooth SIG Announces Architecture to Connect Billions of Devices to the Iot: Supporting Toolkit Enables Developers to for Bluetooth Sensors. Retrieved from: https://www.bluetooth.com/news/pressreleases/2016/02/10/bluetooth-sig-announces-architecture-to-connect-billions-of-devices-to-the-iot.

Kumar, K., P. Sharma and A.K. Singh, 2012. Effect on range of Bluetooth class 1 adapter using external Omni antenna. IJCSC, 3(1): 107-110.

Nagajayanthi, B., R. Radhakrishnan and V. Vijayakumari, 2015. Healthcare IOT-a multilayer security mechanism using linear programmable pre-coded matrix decomposition method. Int. J. Appl. Eng. Res., 10(24): 44554-44563.

Preetha, K.G., 2011. An expanded bluetooth network-a solution to the short range bluetooth communication. In: Wyld, D.C. *et al*. (Eds.), Proceeding of CCSEA, 2011, CS & IT 02, pp: 18-23.

Thorat, S.S., M.K. Sancheti, S.P. Chaudhari, A.B. Nimsudkar and R.P. Jain, 2016. A survey on touch based data transfer using cloud. Int. J. Recent Innov. Trend. Comput. Commun., 3(12): 6776-6779.

Vemuru, B., 2011. Transmit Smart with Transmit Beamforming. Marvell, White Paper, pp: 1-8. Retrieved from: http://www.marvell.com/wireless/assets/ Marvell-TX-Beamforming.pdf.