

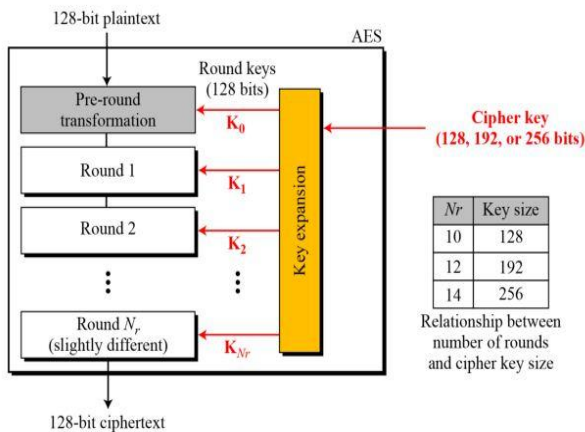


time. Symmetric block ciphers are mostly used for securing data. Famous symmetric block ciphers are Data Encryption Standard (DES), Triple-DES and Advanced Encryption Standard (AES). AES is most widely used cryptographic algorithm for security purposes in consumer and military applications.

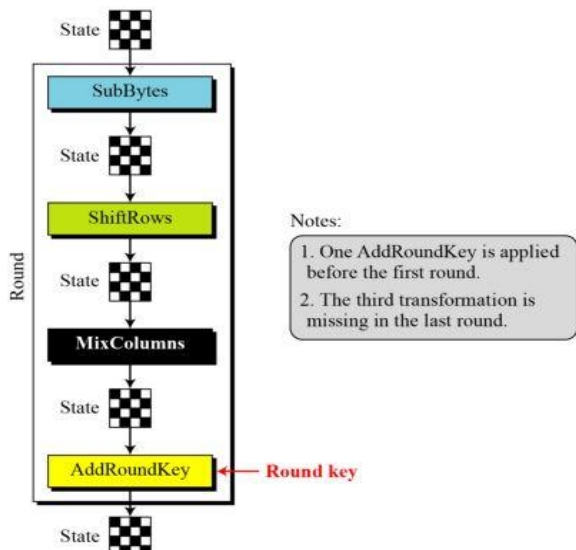
### 3. Advanced Encryption Standard

AES is the symmetric block cipher declared as a standard by National Institute of Standards and Technology of the United States (NIST) [2]. The block sizes used are 128-bits, 192-bits and 256-bits. The operation of AES 128-bits, 192-bits and 256-bits was performed by using 10, 12 and 14 numbers of rounds respectively (see Figure 1). The design is based on a substitution-permutation network (SPN). Following are the features of AES:

- Block encryption implementation
- 128-bit block encryption with 128, 192 and 256-bit key lengths
- Symmetric algorithm that needs only one encryption and decryption key
- Access all around the globe
- No royalties to be paid
- Easy implementation



**Figure 1:** General structure of AES encryption process [6]



**Figure 2:** Structure of single round for encryption [6]

Four types of transformations used in AES:

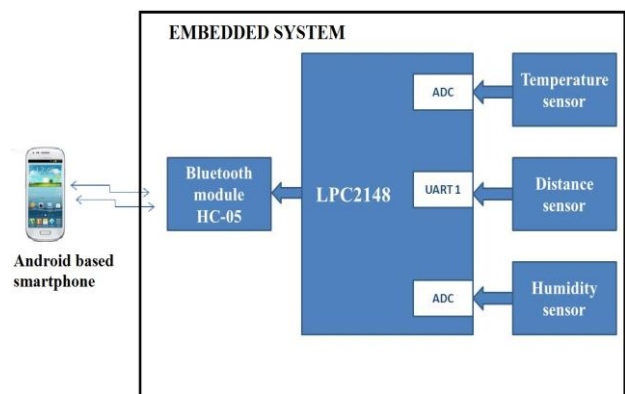
- a) Substitution
- b) Permutation
- c) Mixing
- d) Key addition

The subbytes stage uses a predefined substitution box values to replace the incoming byte value with the corresponding value from the box. The shift rows stage is used to scramble the rows of the 128-bit block. An interbyte transformation is needed that changes the bits inside a byte, based on the bits from the neighboring bytes. Hence there is a need to mix bytes that provides diffusion at the bit level. This is done by the mix column stage. The last stage is the key addition stage in which the 128-bit key is procured from the key scheduling algorithm.

AES is more secure than DES due to its larger key lengths. Moreover no statistical analysis could be done on ciphertext to obtain the plaintext. AES can be implemented in both hardware as well as software. The implementation may include look up tables or software routines. The use of AES is so simple it can be implemented even the cheapest processors and to implement it in software requires no cost.

### 4. System Implementation

The implementation includes an embedded system that has the sensors and actuators interfaced to the central controller. The controller used here is LPC2148 and the parameters that are to be measured are temperature, humidity and distance. For temperature we are using LM35D sensor, for calculating distance ultrasonic sensor is used and for humidity AM1001 sensor is used. The physical values are converted to electrical signals and sent to LPC2148. The controller then does the encryption using AES and 128-bit key. The data is then sent to the Bluetooth module HC-05 which is interfaced to the UART 0 of LPC2148. Figure 3 shows the block diagram of the system.



**Figure 3:** Block diagram of system implementation

Features of LPC2148:

- Flash program memory: 512 kB
- SRAM data memory: 32 kB
- Two 10-bit ADCs with 14 analog inputs
- Operating voltage: 3.0V to 3.6V

- In-System programming
- Two UARTs

The output of LM35D temperature sensor is in voltage and is applied to the AD0.0 pin of LPC2148. The analog voltage is converted to the digital equivalent and is then processed by the controller to create a string that shows the temperature message. This string is then encrypted using AES. Similar to LM25D the humidity sensor provides output in voltage. There is a graph given in the its datasheet which provides humidity percentage equivalent to the sensor output voltage.

The encrypted data is the sent to UART where the HC-05 Bluetooth module is connected. This module works on AT commands and it is configured to be paired with the android smartphone. At the smartphone end the AES decryption process takes place and the encrypted data is decoded to its original form using the same key that was used for encryption.

### 5. Results

The Android application implements AES decryption on the data received from embedded system through Bluetooth.

The following figures show the Android application activities that we have created using Eclipse Luna.

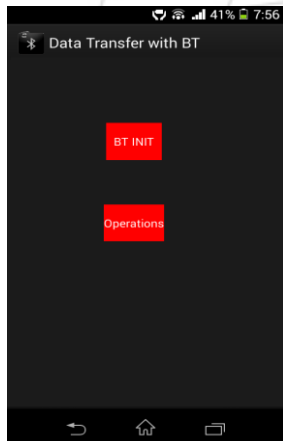


Figure 4: Activity 1

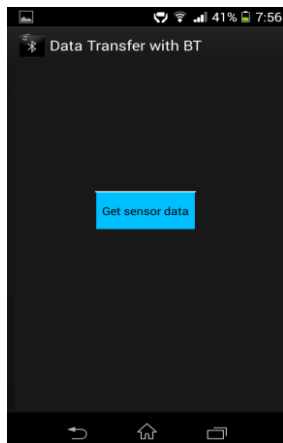


Figure 5: Activity 2

The above activities guide the user through the options such as Bluetooth initialization, operations etc.

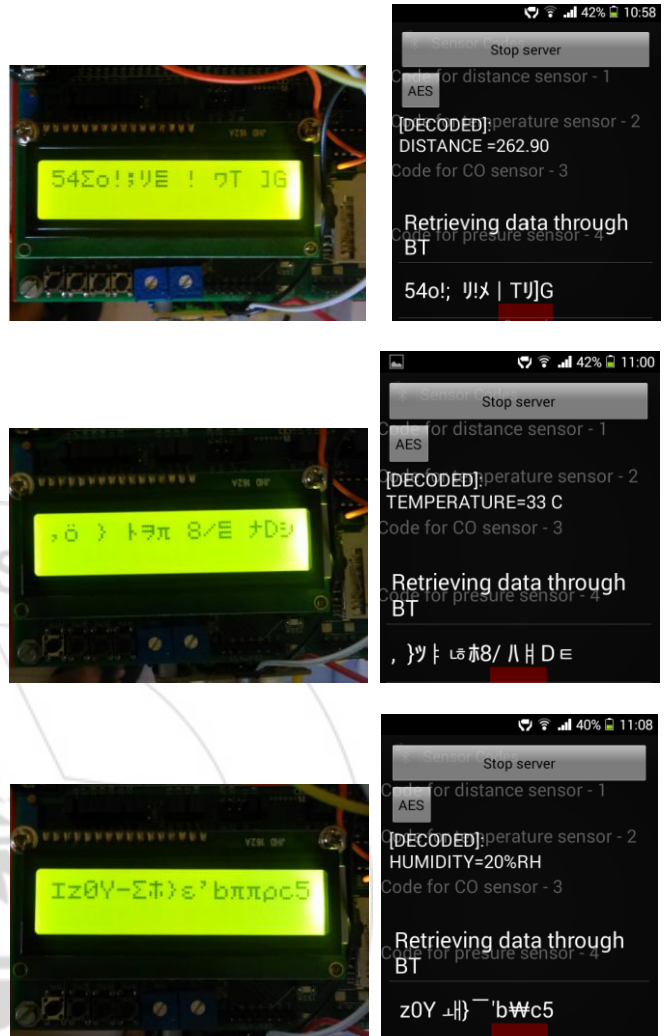


Figure 6: Activities showing the encoded messages from embedded system on left along with the decoded messages in Android application on right for temperature, distance and humidity readings

### 6. Conclusion

We have successfully implemented the AES algorithm on LPC2148 as well as in Android application. The encrypted data from embedded system was sent to the smartphone through Bluetooth which was then decoded in the application. Thus the AES algorithm provides confidentiality, data integrity and authentication. Hence the wireless communication can be said to be secure.

### References

- [1] N. Sloss, D. Symes, and C. Wright, ARM System Developer's Guide, Designing and Optimizing System Software, Morgan Kaufmann, 2004.
- [2] Journal of research of the NIST, volume 106, November 3, May- June 2001.
- [3] NIST, Advanced Encryption Standard (AES), (FIP PUB 197), November 26, 2001.
- [4] T.Ravichandra Babu, K.V.V.S.Murthy, G.Sunil , "AES

Algorithm Implementation using ARM Processor”, 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011.

- [5] W. Stallings, Cryptography and network security.
- [6] AES Available at [www.becs.ac.in/download/doc\\_download/646iss-12-07](http://www.becs.ac.in/download/doc_download/646iss-12-07)
- [7] R. Ashruf et al, Reconfigurable Implementation for the AES Algorithm, Delft University of Technology, Netherlands, 2005

### Author Profile

**Chaitanya P. Kokil** received the B.E. degree in Electronics and Telecommunication Engineering from Marathwada Mitra Mandals College of Engineering, Pune, India in 2012 and is currently pursuing the M.E. degree in VLSI and Embedded systems from MIT College of Engineering, Pune, India.

**Sunil B. Somani** received the M.E. degree in Electronics and Telecommunication Engineering. He has been in the teaching field since last 20 years and specialized in areas such as Advance communication, Microwave engineering and Mobile communication. He is currently working as PG coordinator at MIT College of Engineering, Pune, India.

