iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VI **Month of publication:** June 2021

DOI: https://doi.org/10.22214/ijraset.2021.35358

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Lightweight Cryptography Algorithms for IOT Devices

Vasireddy Vennela[1], Katta Anusha[2], Yara Vasanthi[3], Ms. Nikhila Reddy[4]
[1, 2, 3]*U.G. Student,* [4]*Assistant Professor Dept. of ECE, Sreenidhi Institute of Science and Technology, Hyderabad, Telangana-501301 India*

Abstract: ***Lightweight cryptography is a new concept for securing data more effectively while using fewer resources and providing greater throughput, conservatism, and low battery consumption. Every fraction second, the Internet of Things (IoT), which connects billions of objects, generates massive amounts of data. As the number of devices grows, so does the amount of data generated, and the security of that data becomes a concern. In IoT architecture, gadgets are essentially smaller and low-powered. Because of their complexity, traditional encryption methods are computationally expensive and take many rounds to encrypt, basically wasting the limited energy of IoT devices. However, a less sophisticated method may jeopardise the intended fidelity. There are various lightweight cryptography techniques available, and we choose one of the symmetric encryption techniques known as Advanced Encryption Standard (AES). The speed of this algorithm is six times that of triple DES.***
Keywords: ***Cipher Text, Encryption, Decryption, Symmetric key Cryptography, Asymmetric Key Cryptography.***

I. INTRODUCTION

The “Internet of Things” is the revolution of the future, when trillions of physical items, most of which have limited or no resources, connect with one another without the need for human involvement. In this type of communication, data is crucial. As a result, data must be protected from malicious attacks. Cryptography can help with this. The previous encryption algorithm, Data Encryption Standard (DES), has various flaws, including a short key size and vulnerability to brute force attacks, and thus is unable to guarantee high-level, efficient, and exportable security. A new algorithm known as Advanced Encryption Standard closes these weaknesses (AES). The Advanced Encryption Standard (AES) algorithm is a symmetric block cypher technique that is widely utilized around the world. This technique, which has its own structure for encrypting and decrypting sensitive data, is used in hardware and software all around the world.

II. LITERATURE SURVEY

According to Statista, there were approximately 14.2 million smart homes in the United States in 2016, with that figure predicted to increase to 36.01 million by 2020. We can't take security for granted with this number constantly rising. Attacks on the confidentiality and integrity of domestic systems are common. An attacker could remotely take control of a household to observe the residents' daily activities. Given that the intruder might open the door remotely or operate the equipment in a way that causes physical damage to the residents of the house, this situation may easily turn into a physical attack on the user. This is why, in these home systems, we must design lightweight cryptographic techniques to prevent these assaults. https://portswigger.net/daily-swig/iot is a website that shows attacks on wireless devices all around the world. Sierra Wireless, a provider of Internet of Things (IoT) products, announced on March 20th , 2020 that it had been the target of a ransom ware attack that had halted operations.

III. WORKING

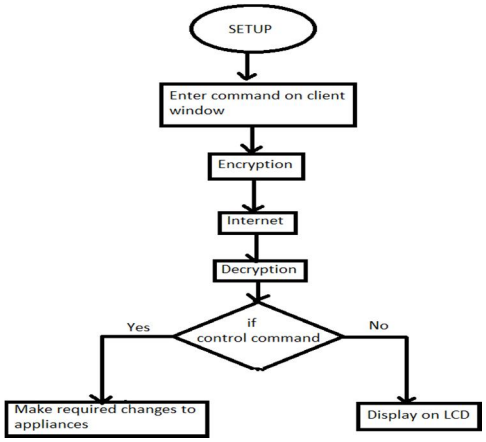


Fig.1 System flow diagram

©IJRASET: All Rights are Reserved

A. 4 different encryption algorithms are implemented and compared on basics of memory consumption (data, program) and execution times (encryption, decryption).
B. Best of those 4 algorithms is used in the building of IOT system. A client-server nodded IOT system is built.
C. The encryption algorithm is used on the data being transmitted from client before transporting via internet. Once the data reaches server node it is decrypted to get the original data.
D. If the data received is an instruction to control appliance it is done accordingly, else it is considered to be a message and is displayed on LCD screen

IV. CIRCUIT DIAGRAM

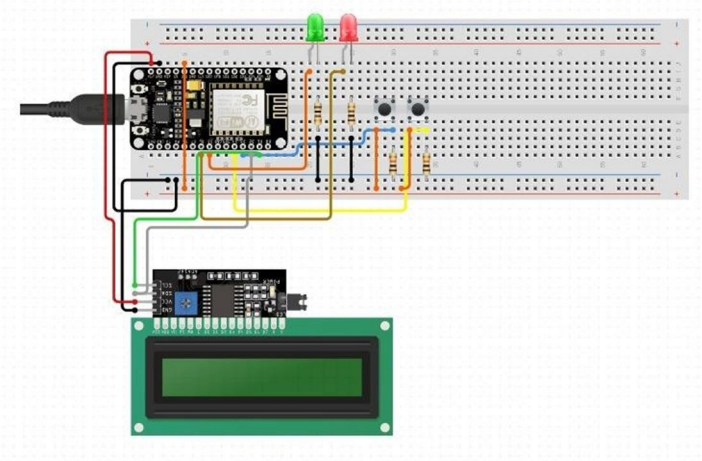


Fig.2 Circuit diagram

A. Nodemcu is given power of 3.3V using type-B USB cable.
B. LCD is connected to i2c module to reduce the number of connections to be given on nodemcu.
C. I2c 4 pins are connected to nodemcu. (SD, SA, Vin-5v, GND)
D. Server code and client code are to be written on Arduino IDE and are to be uploaded to respective nodemcus.
E. Nodemcu is connected to Wi-Fi.
F. Web pages with respective IP address are to be opened to see the status of appliances and message to be transmitted in encrypted form.

V. ALGORITHM

The following algorithms are tried and compared:

1) *AES- 128 (Advanced Encryption Standard):* The Advanced Encryption Standard (AES) is the most popular and commonly used symmetric encryption algorithm available today (AES). 128-bit data, 128/192/256-bit keys symmetric key symmetric block cipher, Triple-DES is stronger and faster. Specifications and design specifications should be provided in full. Software written in C and Java.
2) *DES (Data Encryption Standard):* The prototypical block cypher is DES, which takes a fixed-length string of plaintext bits and turns it into another ciphertext bitstring of the same length via a series of sophisticated procedures. The block size in the case of DES is 64 bits. DES additionally employs a key to modify the transformation, implying that decryption can only be accomplished by those who have access to the encrypting key. The key is supposed to be 64 bits long, but only 56 of them are utilised by the algorithm. Eight bits are utilised simply for parity verification and then deleted. As a result, the actual key length is 56 bits.
3) *Triple DES:* After 1990, the speed of exhaustive key searches against DES started to irritate DES users. Users, on the other hand, did not want to replace DES since changing encryption algorithms that are extensively used and incorporated in major security systems takes a significant amount of time and money. The realistic approach was to alter the way DES is used rather than altogether abandoning it. As a result, Triple DES schemes were adjusted (sometimes known as 3DES).

©IJRASET: All Rights are Reserved

A. Spritz (Advanced RSA)

Asymmetric cryptography is used in the algorithm. Because it employs two independent keys: a Public Key and a Private Key, it is asymmetric. The Public Key is shared with everyone, but the Secret Key, as the name suggests, is kept private. As an example of asymmetric cryptography, consider the following:

A client (for example, a browser) sends the server its public key and requests data. The server encrypts the data and delivers it to the client using the client's public key. This data is received by the client, who decrypts it. Because this is asymmetric, no one other than the browser can decode the data, even if a third party knows the browser's public key.

B. Comparison Of Algorithms

On the basis of Data memory

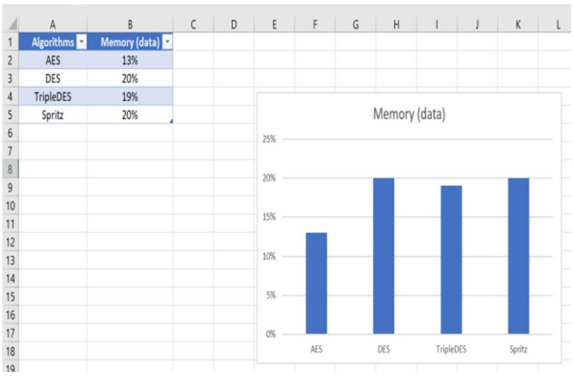


Fig. 3 Data memory consumption

On the basis of program memory

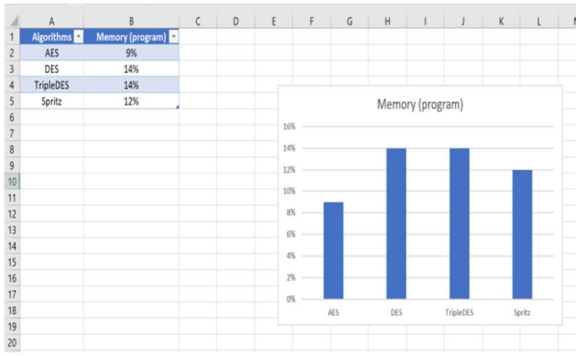


Fig. 4 Program memory consumption

On the basis of Encryption time

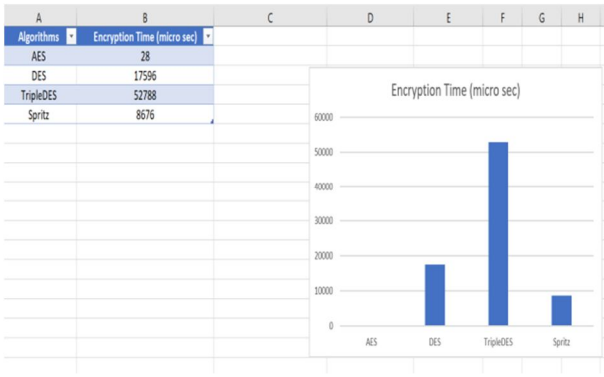


Fig. 5 Encryption time

On the basis of Decryption time

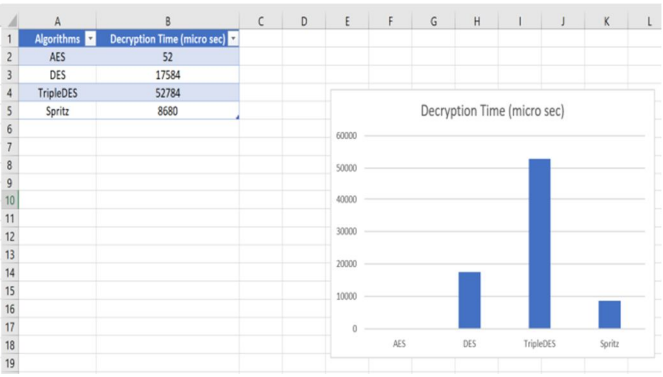


Fig. 6 Decryption time

©IJRASET: All Rights are Reserved

VI. RESULTS

COM7 is serial monitor of client node which sends messages to server node which is shown by serial monitor COM3. The message to be sent has to be entered in text box of COM7 and click “send”. The encrypted message can be seen on both windows.

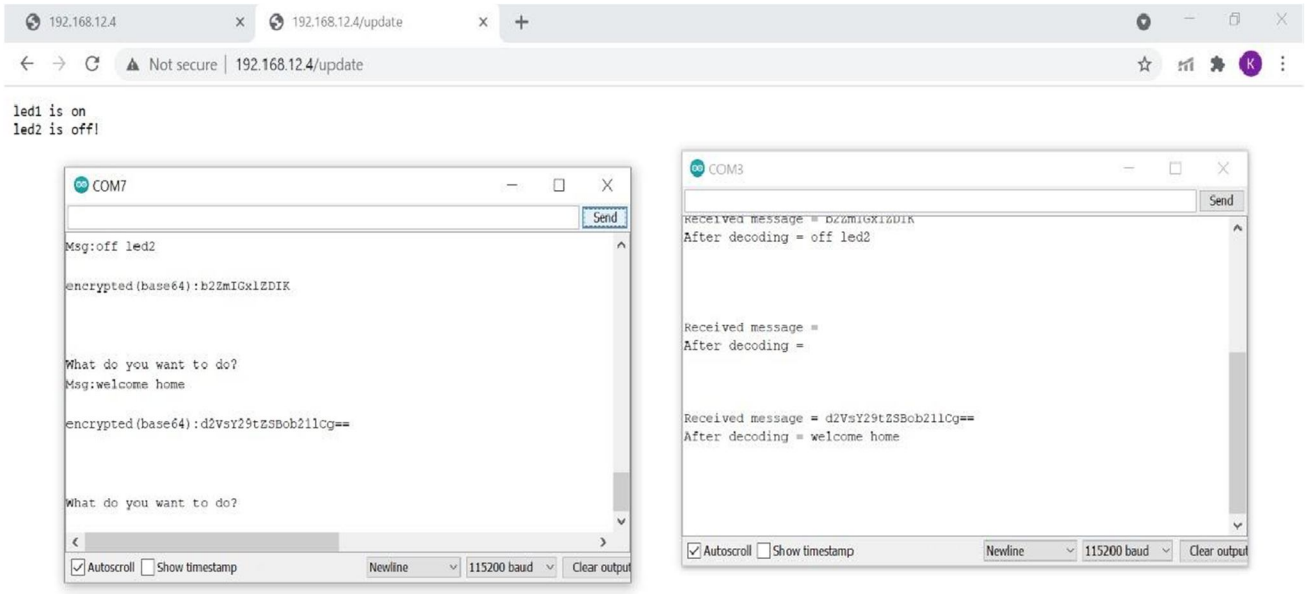


Fig. 7 COM ports

The led1(green LED) is turned on and led2(red LED) is turned off using client node.

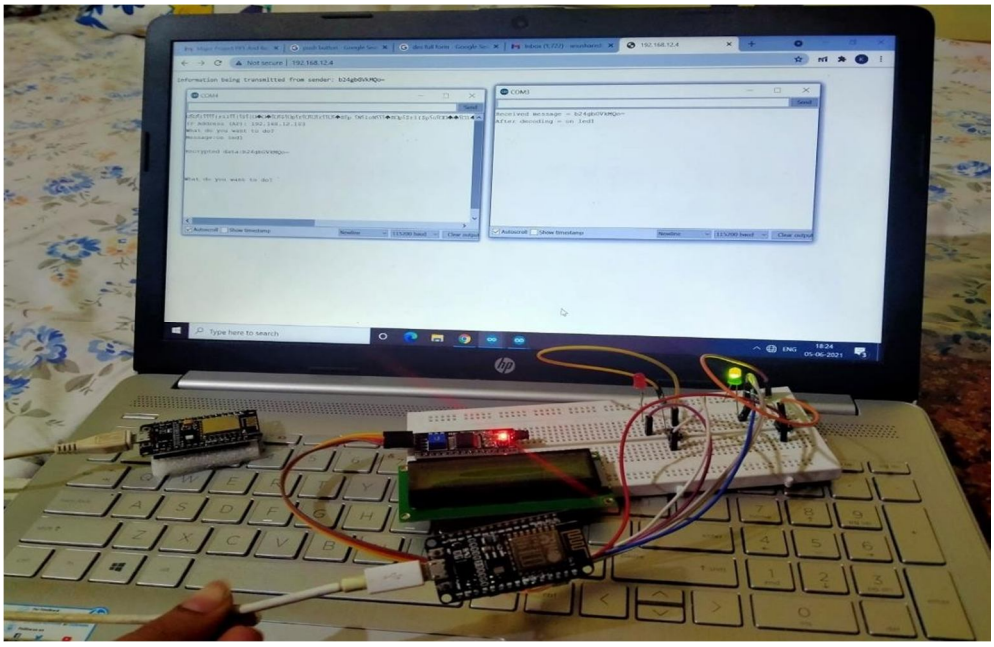


Fig. 8 Hardware setup This is how the message looks on internet (encrypted form)

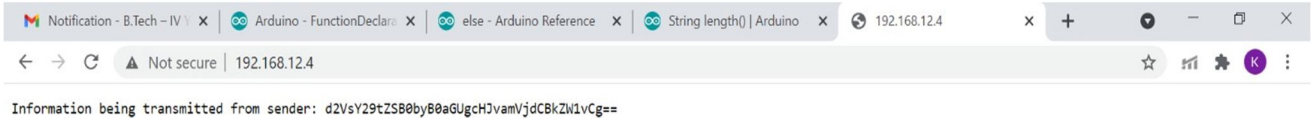


Fig. 9 Message on internet

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VI Jun 2021- Available at www.ijraset.com

Messages other than on/off commands for led lights will be displayed on LCD screen after decryption.



Fig. 10 Message displayed on LCD

The status of lights is visible on website seeing which the commands can be sent accordingly.

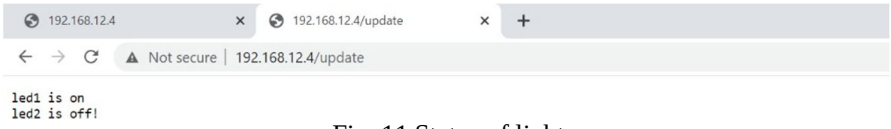


Fig. 11 Status of lights

VII. FUTURE SCOPE

Our research is based on only the implementation of few algorithms. Since it is limited with the comparison of four algorithms, this study doesn't say anything about the performances of others.

Also, we used only one type of electronics platform for our comparative analysis and testing the hybrid scheme. Analysis of other algorithms can be considered as future work.

VII. CONCLUSION

In this research, we proposed a novel method to provide cryptographic security for IoT devices. Because of the inherent limitations of the devices used in IoT in terms of processing power, memory, storage and energy, it is not easy to implement sufficient cryptographic functions.

“If we can safeguard the Internet of Things, it has a bright future.”

VIII. ACKNOWLEDGEMENT

Firstly, we would like to express our gratitude to Sreenidhi Institute of Science and Technology for allowing us to work on this project. We are fortunate to have worked under the supervision of our guide Ms. Nikhila Reddy, Assistant Professor ECE Dept. SNIST. His guidance and ideas have made this project work.

We are thankful to Dr. K. Sateesh Kumar, Assistant Professor ECE Dept. SNIST and Dr. Chattopadhyay, Professor ECE Dept. SNIST for being in charge of this project and conducting reviews.

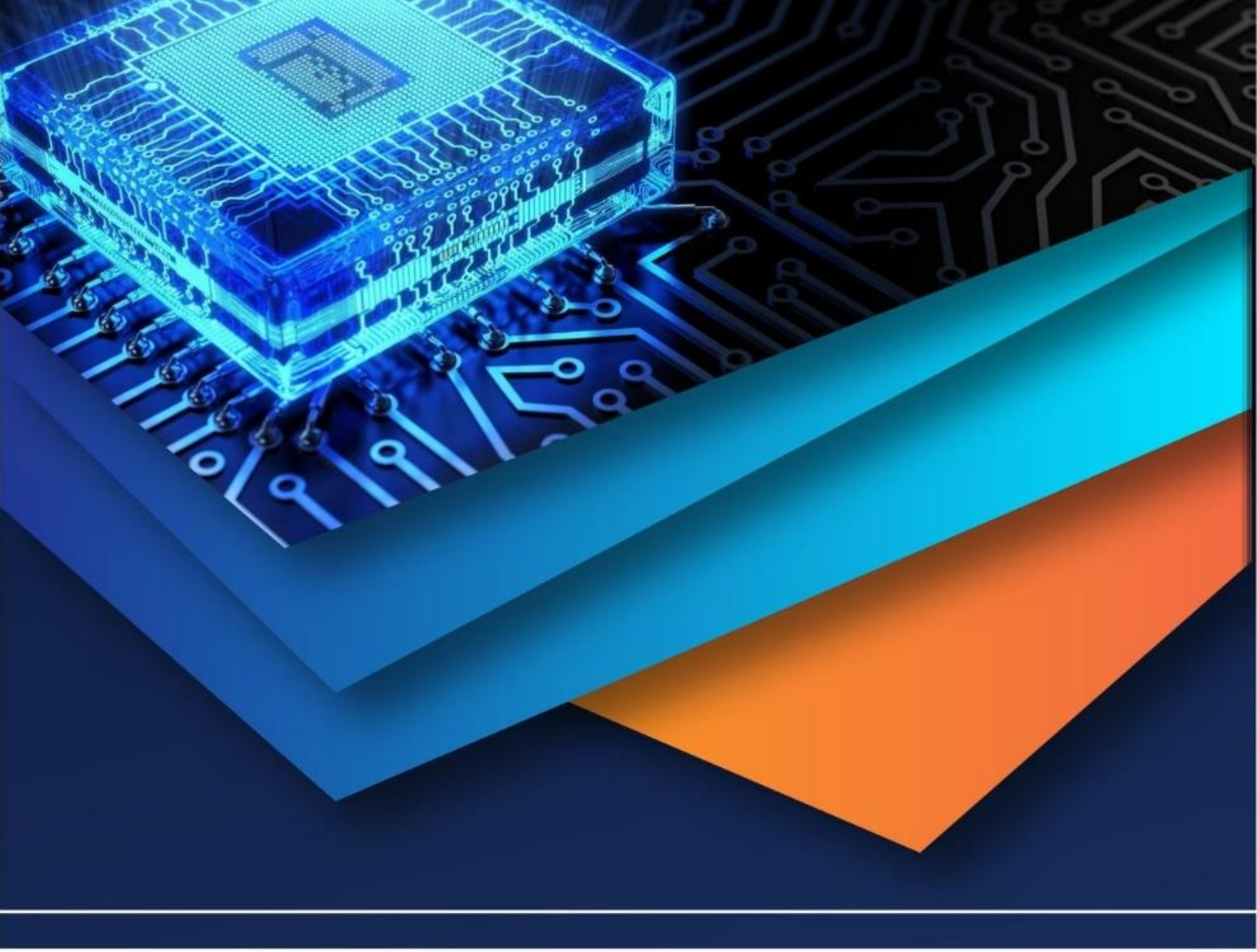
We're also grateful to Dr. S.P.V. Subba Rao, the HOD of Electronics and Communication Engineering [ECE], for providing us with all of the resources we needed to complete this project.

©IJRASET: All Rights are Reserved

REFERENCES

[1] M. Katagi and S. Moriai, "Lightweight Cryptography for the Internet of Things," pp. 7–10, 2008.
[2] https://www.engpaper.com/cryptography-2018.htm
[3] https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography
[4] https://www.academia.edu/49105889/A_Security_Analysis_of_IoT_Encryption_Side_Channel_Cube_Attack_on_SIMECK32_64
[5] U. Kumar, T. Borgohain, and S. Sanyal, "Comparative Analysis of Cryptography Library in IoT," arXiv Prepr. arXiv1504.04306, pp. 1–5, 2015.
[6] A. K. Luhach, "Analysis of Lightweight Cryptographic Solutions for Internet of Things," vol. 9, no. July, 2016.
[7] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," Futur. Gener. Comput. Syst., vol. 49, pp. 104–112, 2015.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)