iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** IV **Month of publication:** April 2020

DOI: http://doi.org/10.22214/ijraset.2020.4035

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 8 Issue IV APR 2020- Available at www.ijraset.com

Exploit DTLS Vulnerabilities & Provide a Novel approach to Protect DTLS in CoAP based IoT

Vraj Shah[1], Snehal Sathwara[2]
[1] *Student M.Tech. in Cyber Security, Department of Computer Engineering, Marwadi University, India*
[2] *Assistant Professor, Department of Computer Engineering, Marwadi University, India*

***Abstract:** In the coming years the Internet of things technology will be very demanding. IoT systems are internet-connected and do a few different things. That senses and transmits data to the cloud. This grows up day by day, and is smarter than humans. One of them is the iot protocol, Constrained Application Protocol. Which is specifically designed for server-client communication. This CoAP is a relatively lightweight protocol. In this paper the main contribution to provide mitigation techniques for UDP Flood attack in Cooja simulator within Contiki's Internet of Things operating system.*
***Keywords:** CoAP, DTLS, DDOS, DOS, IoT, Security, Contiki OS, Cooja Simulator, UDP Flood attack*

I. INTRODUCTION

The Internet of Things (IoT) is defined as a global network that intelligently links all objects, irrespective of hardware, systems or person, with normal and restricted framework protocols and interoperable formats focused on self-configuring technologies for the Internet of Things. Via smart sensing, recognition processing and convincing computation, pursuing the machine and the Internet, IoT was called the Third Wave in the information industry. There are hundreds of IoT enabled protocols. Wireless protocols play an significant role in the growth of IoT, among the other protocols.

Latest developments in Wireless Sensor Network (WSN) technologies and the usage of IP in resource-constrained applications have changed the internet environment significantly. To form the so- IoT trillions of smart objects will be connected to the internet.

IoT requires to combine specific instruments, computers and devices for connectivity that use multiple communications protocols. Some wireless protocols are used in three levels, PHY / MAC, Network / Communications and Application Level. CoAP is one of IETF's most advanced application layers for smart Internet connectivity devices. Since several systems function since parts of cars and buildings with Constrained resources, there is a great deal of variability of power processing, bandwidth connectivity, etc. The lean protocol CoAP is therefore intended as a substitution for HTTP for an IoT application layer protocol and is considered to be an application layer [3].

Application Layer	HTTP, CoAP, EBHTTP, LTP, SNMP, IPfix, DNS, NTP, SSH, DLMS, COSEM, DNP, MODBUS
Network/Communication Layer	IPv6/IPv4, RPL, TCP/UDP, uIP, SLIP, 6LoWPAN
PHY/MAC Layer	IEEE 802.11 Series, 802.15 Series, 802.3, 802.16, WirelessHART, Z-WAVE, UWB, IrDA, PLC, LonWorks, KNX

Fig. 1 The protocols in the different layers are listed

A. Constrained Application Protocol: An overview

CoAP is a RESTfully enabled system application layer protocol which has been developed and used on constrained networks. This was aimed specifically for limited networks, such as 6LowPAN networks. The CoAP was developed to be HTTP-compatible and able to utilize the same methods as HTTP to benefit from current web-based technology i.e. GET, POST, PUT. One distinguishing characteristic of CoAP, though, is the usage of the User Datagram Protocol [RFC 768] (UDP) as a transportation layer protocol instead of a TCP. Nonetheless, because of the UDP's linked nature, the CoAP may have a lightweight redundancy method by separating the CoAP protocol into 2-layers as seen in the diagram below:

Fig. 2 CoAP & HTTP protocols Stack

This is the duty of the Request / Response layer to control resources by specifying methods (i.e. GET, PUT, DELETE, and POST) while the Transaction layer understands the confidentiality function while handling messages and supplies duplicate identification messages. A response could be one of four forms in the Transaction layer: Confirmable (required recognition). Non-Confirmable (needs no ACK). Acknowledgment (Messages to ACK. CON). Reset (message is sent, but was not processable).

B. CoAP Features

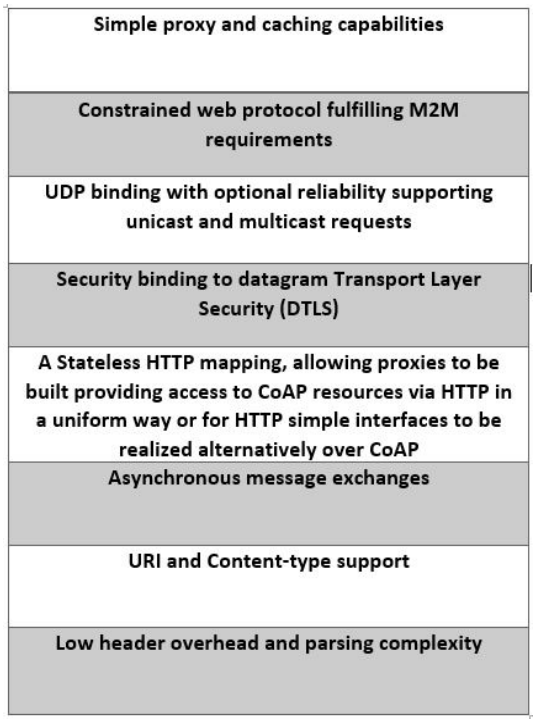


Fig. 3 CoAP Features

With the completion of the CoAP specification, in the future millions of devices are anticipated to be implemented in different technology domains. Such technologies vary from intelligent electricity, smart grid, building management, smart lighting management, industrial control systems, asset tracking, to surveillance of the climate. CoAP will become the regular protocol for communicating devices and promoting IoT applications [3]. To endorse URI (Uniform Resource Identifier) CoAP needs to suggest maximizing datagram duration and satisfying REST protocol. It also needs to have secure UDP protocol dependent communication.

C. DTLS (Datagram Transport Layer Security)

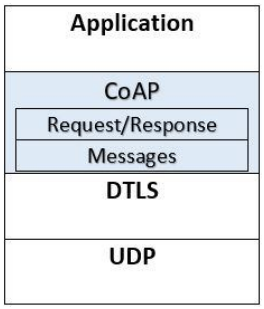


Fig. 4 Datagram Transport Layer Security (DTLS)-secured Constrained Application Protocol (CoAP) architecture.

A restricted application protocol is an HTTP-like request / response data transfer protocol that is used mainly for communicating with restricted devices and/or the use of restricted networks. When safe communication is needed, CoAP uses UDP as a transport protocol and DTLS in the scenarios [Fig. 4]

II. RELATED WORK

They have suggested an interface for the identification and reaction of remote invasions in CoAP-integrations, evaluating their performance in the identification and reaction to attacks and the effect on the memory and resources of restricted wireless sensing systems of protection mechanisms suggested [5].

In this paper, the proposed protocols are investigated and the CoAP implementations are analyzed. The study reveals that some protection standards have not been met by such protocols. In addition, when it comes to deploying IPSec and DTLS using limited devices in IoTs there is a problem of usability. The paper thus argues that a safe version of the CoAP requires a new lightweight, integrated protection mechanism [6].

The reliability of the CoAP protocol is focused on the protection of the DTLS focused on HTTP TLS authentication. With bigger data loads and regular data purchases, DTLS defense is becoming sprawling and CPU heavy. Each of that will be examined as a proper means of managing CoAP protections with respect to point to point or end to end [7]. In this article, they give a detailed evaluation of CoAP's protection through a review of weaknesses and attacks [8].

Based on the associated work, what are the frequent threats centered in CoAP environment and they provide a framework [9, 10] or attack detection [10].

III.OBJECTIVES

DTLS is available to provide protection but it is heavier for the CoAP protocol with that payloads and encryption methods. This also helps the CoAP security architecture to be enhanced.

This work will be aimed at evaluating the numerous attacks, which have the most complete impact on CoAP. And recommended protection mechanism / framework for the CoAP that will make the CoAP protocol quicker, more reliable and more stable in a constrained environment.

IV.METHODOLOGY

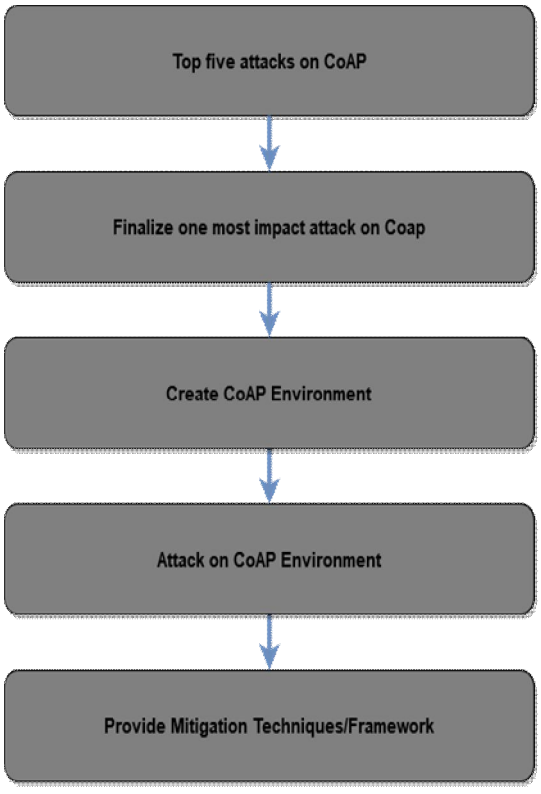


Fig. 5 Flow of research methodology

We have to figure out the most common attacks can be carried out on CoAP. The attacks are DoS, Sniffing, Spoofing, MiTM, Cross-Protocol attacks. After that, we have to finalize one attack which has the most complete effect on CoAP. We have built CoAP Environment and attack on this environment. And lastly we presented the strategies and framework for mitigation [Fig. 5]

V. IMPLEMENTATION

A. Top attacks in CoAP

Whereas methods for authentication have been introduced in CoAP, it suffers from that attacks. In the sub- below, the vulnerabilities were described from the numerous white papers in which the researchers identified these vulnerabilities and possible risks.

1) *UDP flood attack:* A UDP flood is a form of denial of access attack where a large amount of UDP packets are transmitted to a targeted server to overload the ability of the system to handle and reply. The UDP flood is a form of denial of service attack. As a consequence of the UDP floods, the firewall that supports the targeted server may even get overwhelmed and legal traffic is refused services.
2) *MiTM:* Attackers put themselves in a man-in - the-middle attack between two computers (often a web browser and a database server) and capture or alter messages between the two. Then, the attackers will gather details and impersonate one of the two members.
3) *Spoofing:* IP spoofing consists of the development, in order to either mask the sender's identity, or impersonate another computer network, of Internet Protocol (IP) packages that have a changed source. This is an frequently malicious actors tactic used to trigger DDoS attacks on a specific system or the local network.
4) *Sinkhole Attack:* A compromised node or node advertised information in sinkhole Attack for false routes. Drop the packet details after getting the notification packet it. The efficiency of IoT network protocols, like the RPL, is compromised by Sinkhole attacks.

B. Create CoAP Environment in Cooja Simulator

We used Contiki OS with built-in simulator Cooja to test with it. For simulation purposes, we used Sky mote nodes [Fig -6].

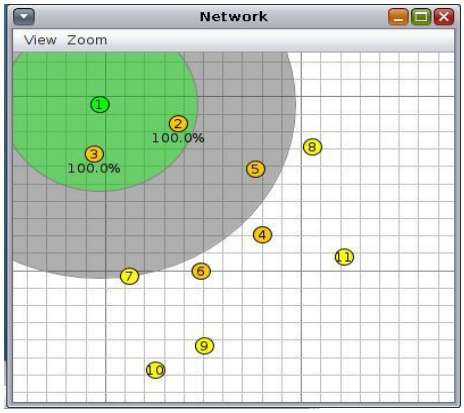


Fig. 6. CoAP Environment in Cooja

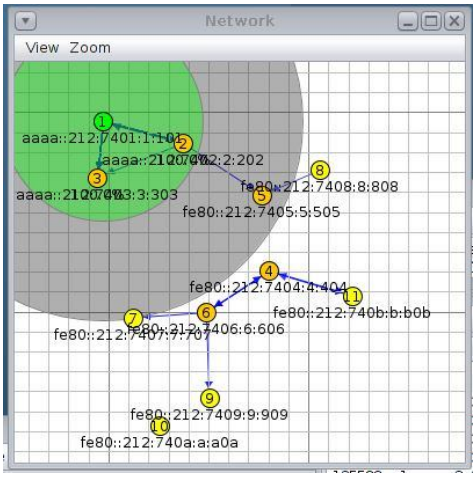


Fig. 7. Packet Routing

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue IV APR 2020- Available at www.ijraset.com

C. Attack on CoAP Environment

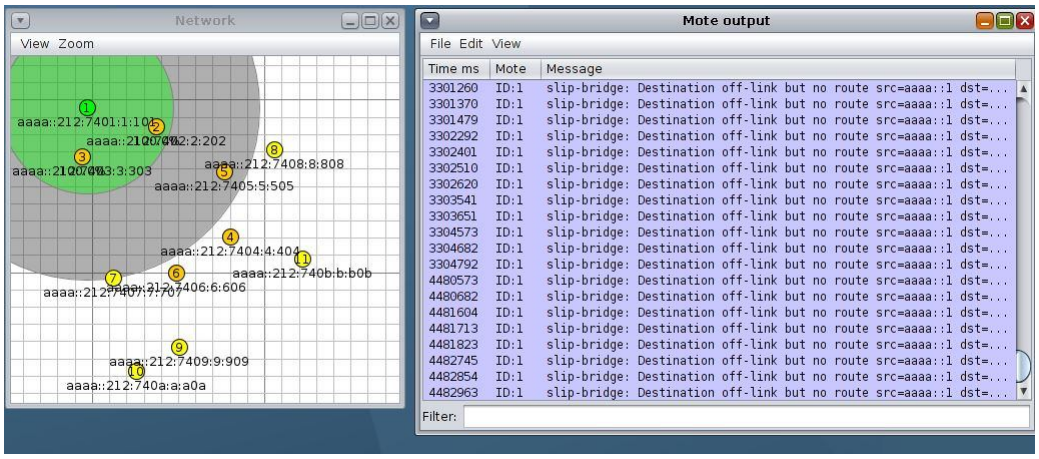


Fig. 8. UDP Flood Attack

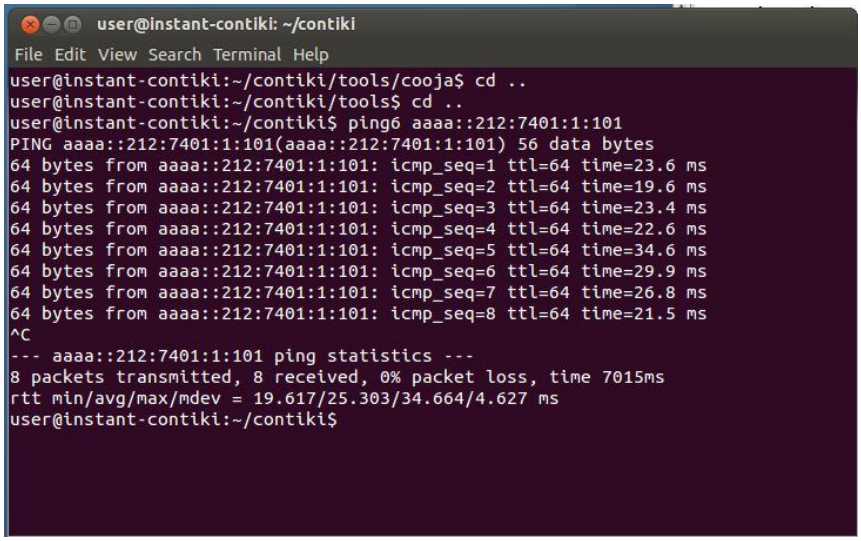


Fig. 9. No packet loss with no threat

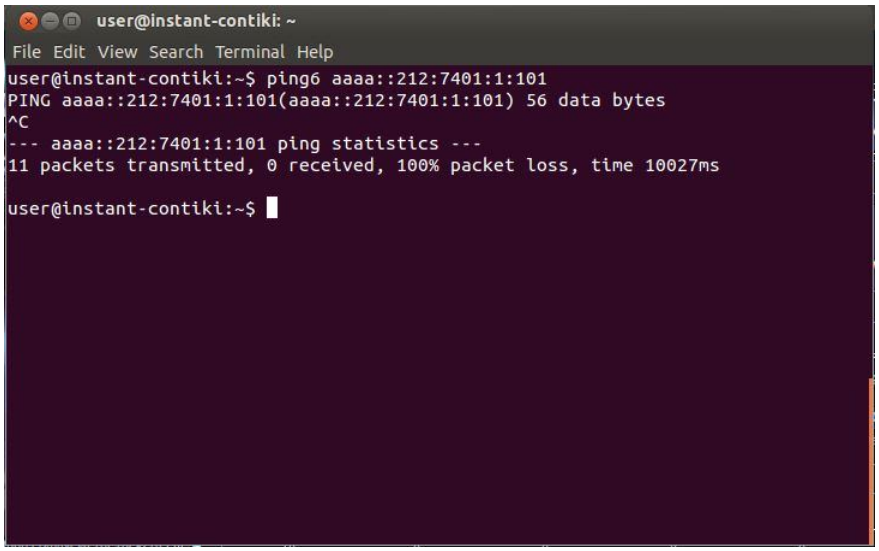


Fig. 10. Packet loss with threat

D. Mitigation Techniques

Attack	Technique & Implications	Defence Mechanism
Flooding Attack, ICMP/ TCP/ UDP/ HTTP/ DNS	May lead to DDoS attack or jamming attack.	Rate-limiting mechanism in Contiki OS.
		SDN based IDS for monitoring activity.
		Dynamic Anomaly Detection module by learning attack behaviour.
Man In The Middle (MITM) Attack	Attacker taps to manipulate or delete information. It can lead to DoS, replay, resource depletion and injection attack	Supervised IDS for attack classification.
Denial-of-Service Attack	DoS, DDoS, Denial of Sleep, SYN Flood, DNS Flood, Ping Flood, UDP Flood, and ICMP Broadcast	SDN architecture to identify DDoS, worm propagation and port scan. IDS coupled provide better security.
		Evasion attacks against ML IDS can be mitigated using Gradient-based approach

Fig. 11. Mitigation Techniques

VI. CONCLUSION AND FUTURE WORK

We have analyzed in this paper the most five common attacks on the Constrained Application Protocol can be done. After this we select one attack that is UDP flood attack and attack on Constrained Environment generated in Cooja simulation in Contiki operating system. And include some strategies for mitigating the attack. In the future, we have work on Intrusion Detection System specially for this attacks in Cooja simulation.

REFERENCES

[1] R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-7.

[2] S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 655-660.

[3] Jain, R., 2020. CSE574S: Wireless And Mobile Networking (Spring 2014). [online] Cse.wustl.edu. Available at: <https://www.cse.wustl.edu/~jain/cse574-14/index.html> [Accessed 23 March 2020].

[4] L. Canuto, L. Santos, L. Vieira, R. Gonçalves and C. Rabadâo, "CoAP Flow Signatures for the Internet of Things," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019, pp. 1-6

[5] Granjal, J. and Pedroso, A. Intrusion Detection and Prevention with Internet-integrated CoAP Sensing Applications. DOI: 10.5220/0006777901640172 In Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), pages 164-172

[6] T. A. Alghamdi, A. Lasebae and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," Second International Conference on Future Generation Communication Technologies (FGCT 2013), London, 2013, pp. 163-168.

[7] Singh, V., 2020. Security Analysis And Improvements To Iot Communication Protocols - Coap. [online] Irjet.net. Available at: <https://www.irjet.net/archives/V6/i7/IRJET-V6I7461.pdf> [Accessed 23 March 2020].

[8] Vraj Shah, "ANALYSIS SECURITY THREATS IN COAP BASED IOT: A SURVEY," International Journal Of Advance Research And Innovative Ideas In Education, vol. 6, no. 1, pp. 695-699, Jan-Feb 2020. [Online]. Available:http://www.ijariie.com/AdminUploadPdf/ANALYSIS_SECURITY_THREATS_IN_COAP_BASED_IOT__A_SURVEY_ijariie11347.pdf [Accessed : 19 February 2020].

[9] P. P. Pereira, J. Eliasson and J. Delsing, "An authentication and access control framework for CoAP-based Internet of Things," IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, 2014, pp. 5293-5299.

[10] P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, 2013, pp. 600-607.

[11] Chen, X. (2020). Constrained Application Protocol for Internet of Things. [online] Cse.wustl.edu. Available at: https://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/ [Accessed 3 Jan. 2020].

[12] Tools.ietf.org. (2020). RFC 7252 - The Constrained Application Protocol (CoAP). [online] Available at: https://tools.ietf.org/html/rfc7252 [Accessed 3 Jan. 2020].

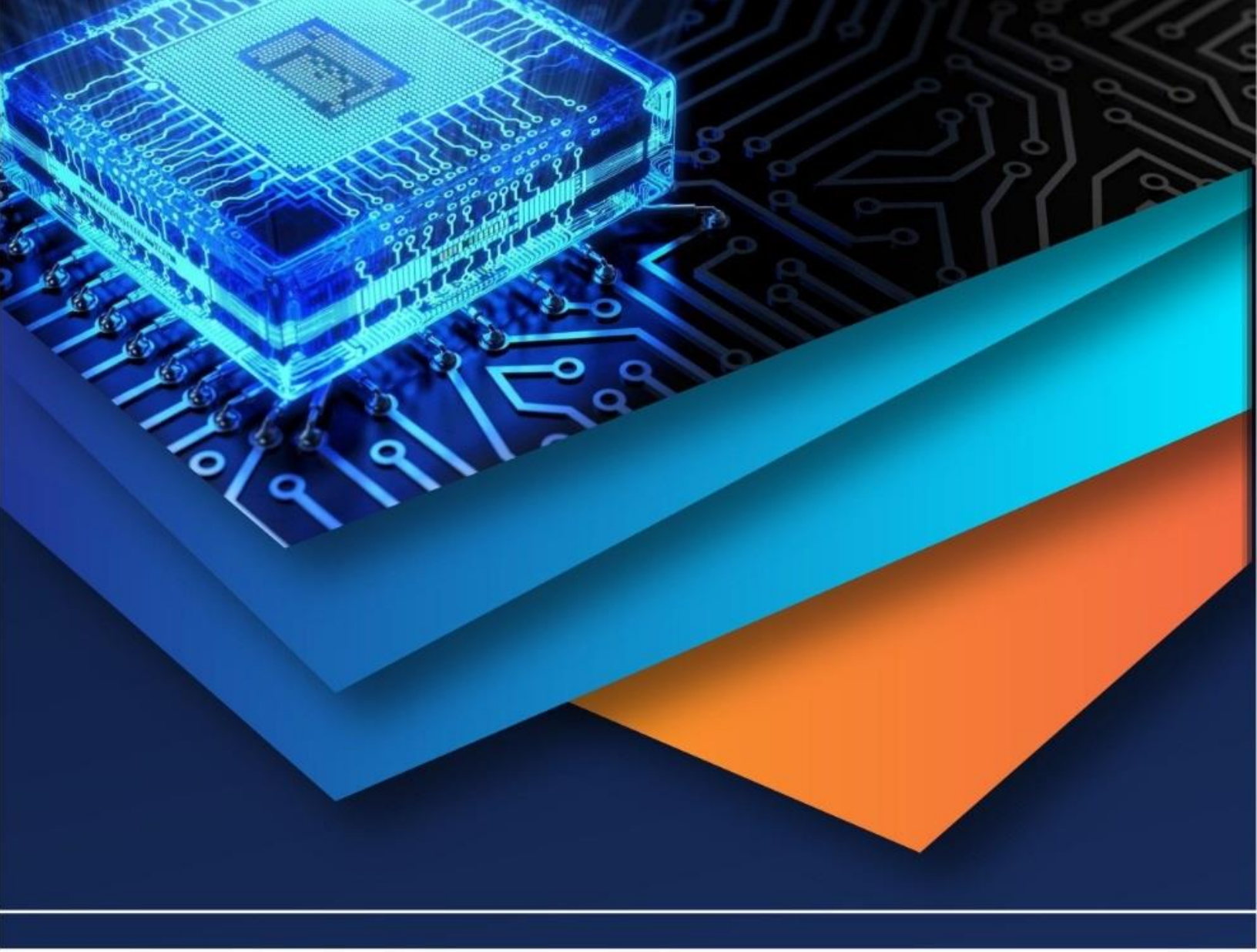
[13] V. Lakkundi and K. Singh, "Lightweight DTLS implementation in CoAP-based Internet of Things," 20th Annual International Conference on Advanced Computing and Communications (ADCOM), Bangalore, 2014, pp. 7-11.

[14] R. K. Kodali, B. Yatish Krishna Yogi, G. N. Sharan Sai and J. Honey Domma, "Implementation of Home Automation Using CoAP," TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea (South), 2018, pp. 1214-1218.

[15] S. Raza, D. Trabalza and T. Voigt, "6LoWPAN Compressed DTLS for CoAP," 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, Hangzhou, 2012, pp. 287-289.

[16] T. A. Alghamdi, A. Lasebae and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," Second International Conference on Future Generation Communication Technologies (FGCT 2013), London, 2013, pp. 163-168

[17] Cimpanu, C. (2020). The CoAP protocol is the next big thing for DDoS attacks | ZDNet. [online] ZDNet. Available at: https://www.zdnet.com/article/the-coap-protocol-is-the-next-big-thing-for-ddos-attacks/ [Accessed 28 Jan. 2020].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY