iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30485

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 VII July 2020- Available at www.ijraset.com

Securing Data in Internet of Things (IoT) using Cryptography and Steganography Techniques

Jyoti Laxman Kuri[1], Dr. Mohamed Rafi[2]
[1]*P.G. Student,* [2]*Professor And Supervisor, Department of Studies In Computer Science and Engineering, University B D T College Of Engineering, Davanagere, Karnataka, India*

Abstract: ***The Internet of Things (IoT) could also be a network of connected vehicles, physical devices, software, and electronic things that facilitates data exchange. The aim of IoT is to provide the IT-infrastructure for the secure and reliable exchange of "things." safety of this knowledge could be a difficult task; but, security challenges will be lessened with cryptography and Steganography techniques. These techniques square measure crucial once addressing user authentication and knowledge privacy. Within the planned work, the elliptic Variety Galois cryptography protocol is introduced and mentioned. During this protocol, a cryptography technique is employed to encode confidential knowledge that came from totally different medical sources. Next, a Matrix XOR coding Steganography technique is employed to embed the encrypted knowledge into an occasional complexes image. The planned work additionally uses associate optimization algorithmic rule is a known as adaptation Firefly to optimize the option of canopy blocks among the image. Supported the results, varied parameters square measure evaluated and compared with the prevailing techniques. Finally, the info that's hidden within the image is recovered and is then decrypted.***
Keywords: Internet of Things (IoT), confidential data, Cryptography, Steganography, Data security.

I. INTRODUCTION

The Things Internet (IoT) can be an interconnected vehicle, physical device, software and electronic device network that enables the exchange of knowledge. IoT's aim is to create a secure and reliable "Things" exchange infrastructure. IoT 's design comprises mainly of the mix of sensors / actuators, RFID tags and networking technologies. The IoT does however explain that the Internet can integrate an extension of physical things and devices so that these objects can join forces Communicate with each other in order to achieve shared goals. The Internet of Things comprises mostly of very low materials squarely measure the cooperative shrewd things. The Internet of Things limitation encompasses energy, properties and power of the machine.

Although Internet of Things devices have made life more easy, the protection of these devices has been paid very little attention. The main aim of developers at the moment is to increase devices' capabilities, with little stress on device protection. The data transmitted via the IoT network is in danger of being targeted. Such material is important to preserve the user's privacy. There is no safety of the information, and therefore personal information can simply be hacked from the system. There is a violation of the information. Identification and authentication include a number of necessary IoT ideas. These square ideas measure interconnected to all alternatives, such as crypto graphical functions which are necessary to confirm that the knowledge is transmitted to the right equipment and whether or not the supply is certain. A hacker simply communicates to any device with the lack of authentication.

Whenever two devices interact, information between them is transferred. Knowledge may often be highly delicate and confidential. There is therefore a wish for the cryptography of information, once this delicate knowledge moves from device to device over the IoT network. Together, cryptography helps to protect intruders' knowledge. Details may be easily authenticated by cryptography, i.e. by converting a simple and unintelligible document to easy code. Cryptography square primary objectives measure privacy, completeness, non-repudiation and authentication. Curve Elliptic cryptography (ECC) is one in all the crypto graphical Algorithms used in the work planned. Error correction code may be a crypto graphically supported public keys over finite fields to support the algebraic structure of the elliptical curves.

Additionally, In order to achieve additional safety to the information, a further technique, known as Steganography, is used for the planned work. Steganography hides encrypted messages so that no one can suspect, even in place I, that the corresponding grade encrypted message exists. Cryptography of information takes place using typical encryption techniques in fashionable digital Steganography. Then a special rule can be used as an insert into redundant data, such as a jpeg image, {the knowledge of information} in a file format. The work planned uses Steganography from Matrix XOR to create extra safety. The picture block is designed using the Firefly law implementation, where secret information is concealed from an immense picture block during an elite phase.

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

In Virtualization-based security middleware for the IOT. Authors W. Daniels [1] Introduced security micro visor (SμV) middleware, that uses code virtualization and assembly level code verification to produce memory isolation and custom security.
In Energy-efficient datagram , Authors Banerjee [2] provided energy-efficient data graph transportation layer protection (eeDTLS) which could be a low energy option on data graph transport layer safety (DTLS).
In massive information counterintelligence for health care business four.0, Authors Manogaran [3] planned a system during which medical detector devices area unit embedded within the Body to gather patients ' health steps. Big shifts in concentrations, pressure levels, heart rate, glucose and signals over and outside the sensor region, which generate an warning AN with health details transmitted by a wireless network. Wireless information is provided to the doctor. Wireless information. This approach utilizes a huge management protection system to safeguard large volumes of company knowledge.
In Cloud-based malware detection with reversible sketch for resource-constrained IOT, Authors H. Sun [5] planned Cloud Eyes, an anti-malware program focused on the cloud. The program equipped the users inside the IoT network with cost-effective and reliable monitoring services.
In Configurable reliable distributed information storage systems for IOT to confirm security, Authors Chervyakov [6] provided an information storage theme for the smallest amount likelihood of information Redundancy, data loss as well as encryption and secret writing speed that deals with completely different targets, Loads of work and storage features. This research shows that if RRNS is correct, then it is not correct require just improved protection and efficiency, but also allows to improve the process pace of encryptive knowledge. The findings of this analysis is right. The application on IoT Application usually need additional information than ancient applications.
In light-weight weight secure CoAP for the IOT, Authors Raza [7] given light-weight Safe IoT CoAP (Lithe), which supported the creation of a totally unique theme for DTLS header compression, with 6LoWPAN to reduce energy use. Moreover, the DTLS compression header theme does not jeopardize safety. Vu'cini'c et al., the anticipated architecture for the protection entity (OSCAR), is the IoT-end-to defense framework. Honor focuses on a framework that exposes payload security to the protection of AN objects.
In light-weight break-glass access management system for health care IOT, Authors Y. Yang [8] planned the light-weight The Li BAC system, whereby medical files will be encrypted in 2 ways, is break-glass access control (1) access based on attributes, 2) bro-glass access.
In Usual, if the set of attributes complies with the access policy in a medical file, medical staff will decode and access information. A break-glass access mechanism is used in the event of an emergency to bypass a medical record access strategy to provide emergency medical help or rescue staff with timely access to information. For the health and medical industries, the security and confidentiality of knowledge sent over the IoT network may be a priority.
In An economical Steganography approach for safeguarding communication within the IOT crucial infrastructures,
Authors Bairagi [9] developed 3 strategies for concealment info so IoT network communication with the help of Steganography will be maintained. With the assistance of borderline distortion (LSB) and knowledge signs can be even employed, the info is hidden within the most profound layer of the image. When put next to the particular method, this system improved physical property and talent.

III. PROPOSED APPROACH

1) *Elliptic Galois Cryptography and Steganography Protocol:* The proposed system proposes the elliptic Galois cryptography (EGC) protocol for protection against data infiltration during transmission over the IoT network. In the proposed work, different devices in the IoT network transmit data through the proposed protocol as a part of the controller. The encrypted algorithm within the controller encrypts the data using the EGC protocol and then the encrypted and secured message is hidden in layers of the image, with help from the Steganography technique. The image can then be easily transferred throughout the Internet such that an intruder cannot extract the message hidden inside the image. Initially, the EGC technique encrypts confidential data. Subsequently, the encoded secret message is inserted within the image by the XOR Steganography technique. Next, an optimization algorithm called the Adaptive firefly .

©IJRASET: All Rights are Reserved

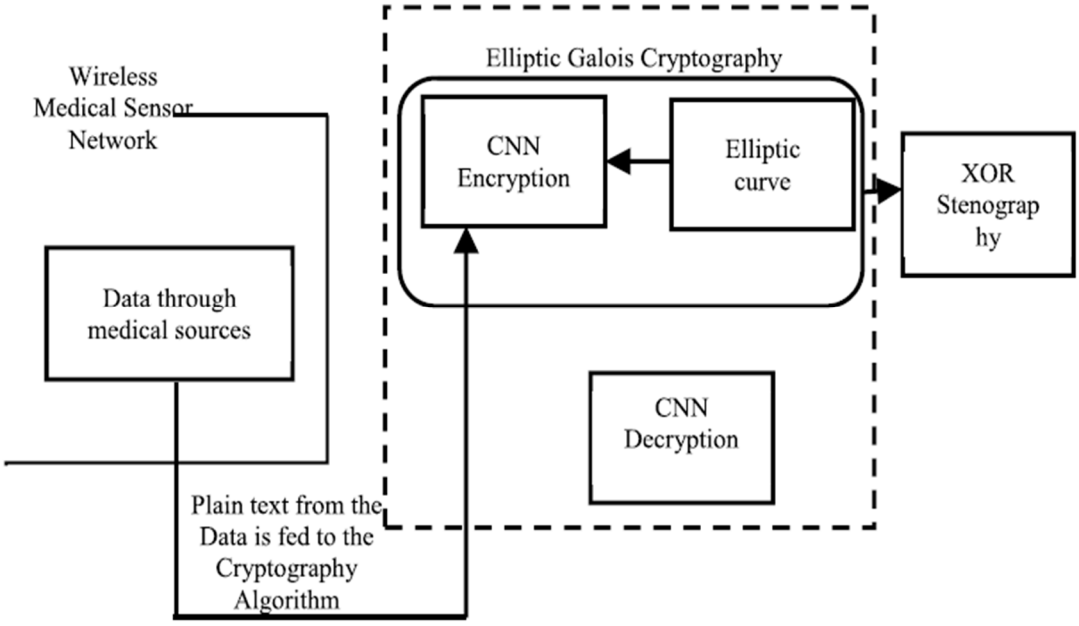


Fig: EGC

2) *Elliptic Galois Cryptography:* ECC, commonly known as the public key encryption technique, is based on elliptic curve theory. The keys are generated by using the properties of elliptic curve equations instead of traditional methods. The proposed work uses EGC. For improving the efficiency of calculations and to reduce the complexities of rounding errors, the elliptic curve over the Galois field (*Fa*) is used. The value of the Galois field must be greater than one.

3) *Matrix XOR:* Matrix XOR is a technique for hiding encrypted data in which the encrypted data is hidden inside the H.264 video file .For this technique, the Firefly optimization technique is used to optimize the blocks of the image. With the help of this optimization technique, block selection among the whole image is possible. The proposed OM-XOR Steganography technique .The initial image is tiled and the secret data is hidden on the cover block with the help of Adaptive Firefly optimization. The tiled image is recombined and decoded. Finally, the encrypted message is decoded by using the secret key.

a) *Step 1 (Permutative Straddling):* When there is no need to use the full size to hide the encrypted message, the fragment of the image remains unused. Permutative straddling is used to eliminate this problem. This technique scatters the secret message over the complete carrier medium; i.e., over the complete image. Permutation depends on a key-based password. If the user has the correct key, the same permutation can be repeated.

b) *Step 2 (Encoding):* There are many algorithms for embedding secret information into an image block. By introducing the Matrix XOR encoding technique, the proposed work enhances the embedding efficiency. The conversion of triple*(f , k, g(i))* to quad*(e, k, g(i))* and the compression of the encrypted message enhances the efficiency of this technique. The Matrix XOR technique embeds the *g(i)* chaotic sequence (secret data) in the optimized image block (cover block). In this process, the one-bit block from the cover block is replaced with the encrypted information block. The one-bit embedding process is carried out using the following equation:

$$M_e = D + C$$

c) *Step 3 (Adaptive Firefly Optimization):* Adaptive Firefly algorithm is contains some standard rules.

- All the fireflies are unisex so that all fireflies are attracted to each other.
- Attractiveness between the fireflies is proportional to their brightness; thus, a less bright firefly will move toward a brighter one. With increased distance between fireflies, both the attractiveness and brightness decrease.
- The brightness of a firefly is determined by the landscape of the objective function. Two important issues persist in the Firefly algorithm: a) formulation of the attractiveness and b) the variation of light intensity.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

IV. EXPERIMENTAL RESULTS

A. Database Description

Some official videos, such as MPEG 2 and MPEG 4 help to achieve a high compression ratio. Although high-performance efficiency is achieved, there is a loss in the compression ratio . This problem is solved with supreme progressive film coding model up-to-date. H.264 MPEG-4 is similarly used for this process and the video quality of this H.264/AVC is H.264, and each video has 30 frames/s. Video resolution is 304 × 204 pixels. The cover block image, which is the converted frame for the H.264/AVC video, is depicted in Fig. 4(a). Fig. 4(b) corresponds to the Stegno image in which medical data is hidden in the profound layer of the cover block. Thus, with the help of the proposed method, the medical data of the patient is securely hidden within the image. The data that is hidden with the proposed method cannot be extracted by any unauthorized person since only the ECC secret key can retrieve the original data.



(a)



(b)

Fig. 4. Matrix XOR Stegno image and cover image. (a) Cover image. (b) Stegno image.

B. Parameter Evaluation

For showing the efficiency of the proposed EGC system, carrier capacity, peak signal to noise ratio (PSNR), mean square error (MSE), and time complexity were evaluated. The results of all these parameters were compared to some of the existing methods, such as LSB Steganography, FMO Steganography, and optimized modified matrix encoding (OMME) Steganography. Various graphs have been put-up to efficiently show the comparison between the proposed work and the existing methods. The parameters are evaluated as follows.

©IJRASET: All Rights are Reserved

1) *Mean Square Error:* MSE is the amount of similarity and the range of distortion in an image and it also helps in the measurement of the amount of reliability

$$MSE = \frac{1}{N} \sum^{n}_{i=X,Y} (X - Y)\,2$$

N is the total pixel within the image, X is the initial image, and Y is the final Stegno image.

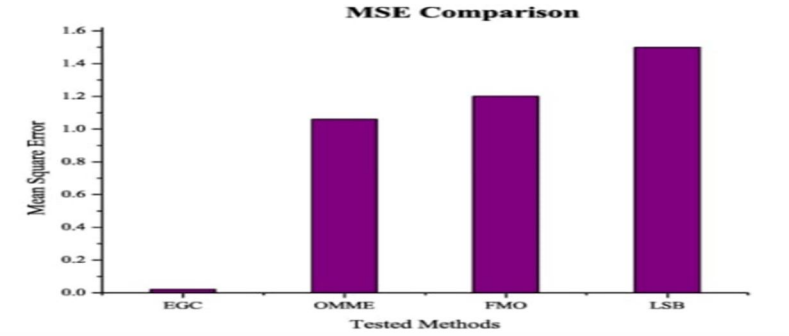


Fig . 1. Mean Square Error analysis

2) *Peak Signal to Noise Ratio:* PSNR calculates the invisibility of the image. PSNR can also be used for dynamic range images

$$PSNR = 10 \log 10 \frac{255}{MSE}.^{2}$$

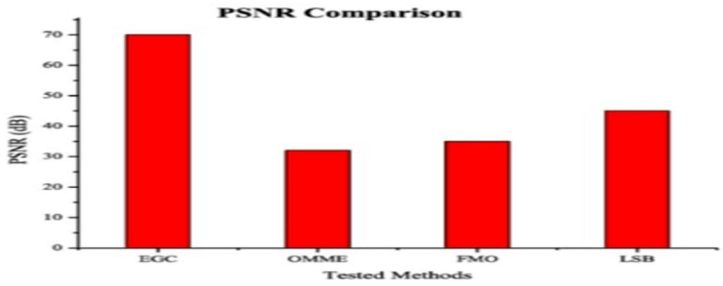


Fig. 2. Peak Signal to Noise Ratio analysis

3) *Carrier Capacity (C):* Carrier capacity is the ability of the system to hide encrypted data inside the cover block. The value of carrier capacity is directly proportional to the performance .

$C = Total\ number\ of\ secret\ bits\ /Number\ of\ bits\ in\ the\ cover\ block.$

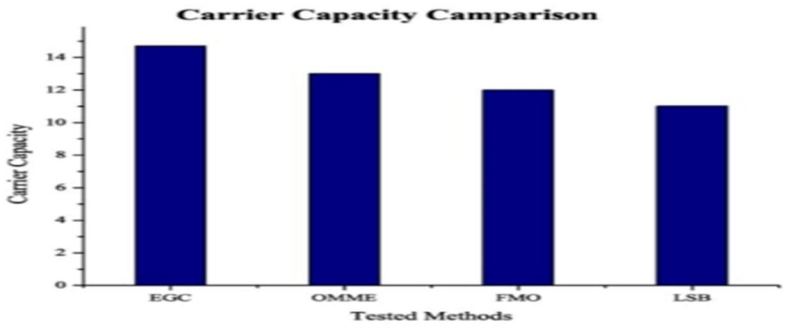


Fig. 3. Carrier Capacity analysis

Carrier capacity is the other name for hiding capacity and is measured in terms of bits per pixel (BPP).

©IJRASET: All Rights are Reserved

4) Time Complexity: Time complexity is the amount of time taken between the encryption and decryption process. To increase the efficiency of the system, time complexity must be lowered. Comparative analyses are shown in Figs.

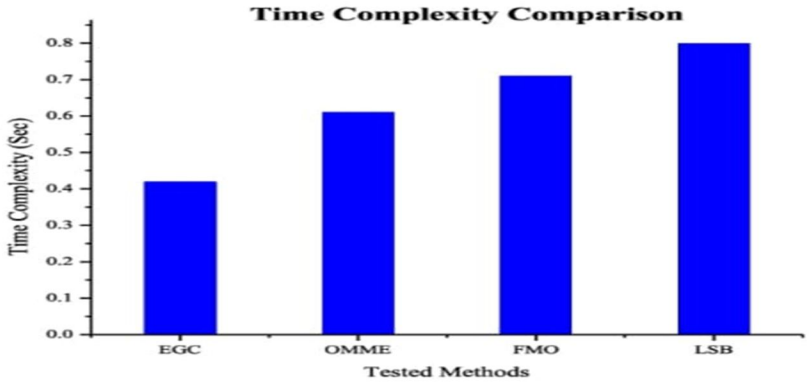


Fig. 4. Time Complexity analysis

C. Parameter Comparison

Sl. No	Parameters	Methods			
		EGC	OMME	FMO	LSB
1	Mean Square Error	0.02	1.0	1.2	1.5
2	Peak Signal to Noise Ratio	70	30	40	45
3	Carrier Capacity	15	13	11	10
4	Time Complexity	0.4	0.6	0.7	0.8

The EGC protocol gave better performance regarding carrier capacity, PSNR, MSE, and time complexity as compared to other techniques, such as LSB Steganography, FMO Steganography, and OMME Steganography. As depicted in Figs. 2 and 3, the MSE and time complexity of the proposed EGC protocol is very low, as compared to existing methods.

The proposed protocol yielded better PSNR performance as compared to LSB, FMO, and OMME (32.42%, 45.62%, and 52.24% better performance as depicted in Fig. 2. Fig. 3 shows that the proposed protocol yielded better carrier capacity performance as compared to LSB, FMO, and OMME (0.33%, 16.35%, and 9.36% better performance, respectively). Therefore, overall the proposed method is well optimized and yielded better results when compared to the existing protocols.

V. CONCLUSION

In order to protect data during IoT transmission, the EGC protocol generated a high level of data security. The proposed EGC protocol improved security with the latest ECC on the Galois region. Because of the increased integration performance, advanced capabilities for hiding data are feasible. Due to the suggested specification and configuration of the adaptive firefly, some volume of data can be transferred conveniently across the IoT network safely within the deep picture layers. The efficiency of the embedding, the PSNR, carrier capacity, time complexity and the SSE are evaluated using parameters.

©IJRASET: All Rights are Reserved

REFERENCES

[1] W. Daniels *et al.*, "SμV-the security microvisor: A virtualisation-based security middleware for the Internet of Things," in *Proc. ACM 18th ACM/IFIP/USENIX Middleware Conf. Ind. Track*, Dec. 2017, pp. 36–42.

[2] U. Banerjee, C. Juvekar, S. H. Fuller, and A. P. Chandrakasan, "eeDTLS: Energy-efficient datagram transport layer security for the Internet of Things," in *Proc. GLOBECOM IEEE Glob. Commun. Conf.*, Dec. 2017, pp.1-6

[3] G. Manogaran, C. Thota, D. Lopez, and R. Sundarasekar, "Big data security intelligence for healthcare industry 4.0," in *Cybersecurity for Industry 4.0*. Cham, Switzerland: Springer, 2017, pp. 103–126.

[4] H. Sun, X. Wang, R. Buyya, and J. Su, "CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices," *Softw. Pract. Exp.*, vol. 47, no. 3, pp. 421–441,2017.

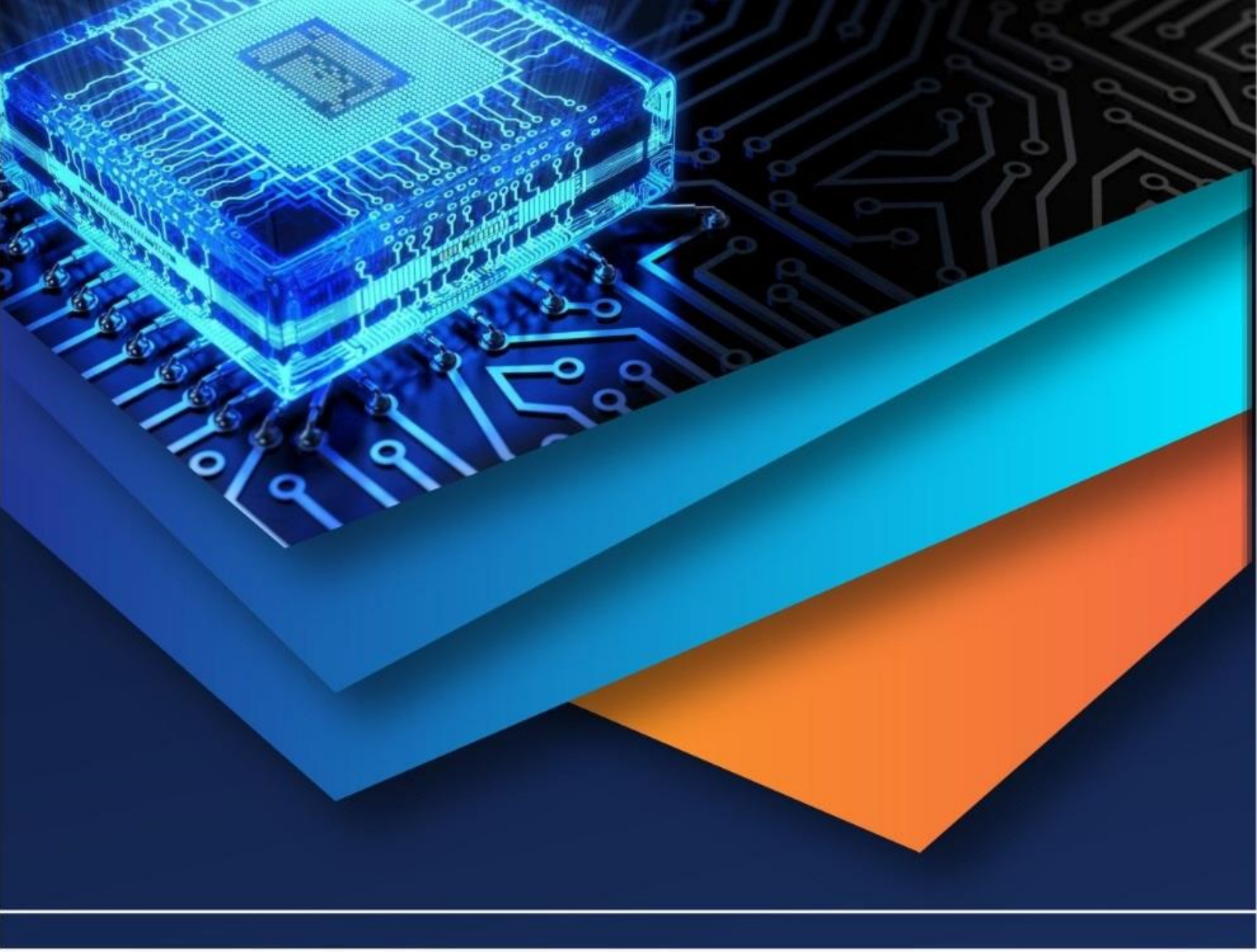
[5] N. Chervyakov*et al.*, "AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security," *Future Gener. Comput. Syst.*, vol. 92, pp. 1080–1092, Mar. 2019.

[6] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol. 1, no. 10, pp. 3711–3720, Oct. 2013.

[7] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3610–3617, Aug. 2017.

[8] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Security J. Glob. Perspective*, vol. 25,nos. 4–6, pp. 197–212, 2016.

©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)