iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** IV **Month of publication:** April 2021

DOI: https://doi.org/10.22214/ijraset.2021.33728

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 IV Apr 2021- Available at www.ijraset.com

Security and Privacy Preserving of Data using CP-ABE Scheme

Ms. Swati Gajarlewar[1], Prof. A. A. Nikose[2]
[1, 2]*Department of computer science and engineering, Priyadarshini Bhagwati College of Engineering, Nagpur, India*

Abstract: ***Due to the rapid development of new technologies, data security is one of the big challenges in today's world. Particularly, in the healthcare field, a large amount of data is generated every day. To maintain the patient personal records by manually and handling them, is not very sure, and Also avoiding the paper-work in the health care industry is not a good practice. As more records are stored electronically they need security and confidentiality. Different methods were proposed to prevent both internal and external threats in the healthcare industry. In healthcare industries record are extremely sensitive; therefore requires more security and privacy when storing and sharing of those records. The security as well as the privacy of sensitive health records are the major challenges in health care industries. To prevent unauthorized access to the healthcare records the user should be authenticated to get access to the records. To secure the data, cryptography techniques are used. The first is symmetric key encryption techniques which use only one key for both encryption and decryption of the data. Their design simple but can be easily cracked by using brute force attacks. On the other hand, the second is asymmetric key encryption techniques which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric key encryption ones but lack in time efficiency. In our proposed system different access control mechanisms are used to provide security and confidentiality on healthcare records.***

Keywords

I. INTRODUCTION

Data is continuously exchanged over different networks. It is correct to say that a huge part of the data is private or confidential which demands stronger techniques of encryption. There are two commonly used cryptography techniques for securing the data that is transmitted over the network, these are encryption and decryption. Therefore, there are a lot many encryption-decryption systems to encrypt and decrypt the transmitted information. The first is symmetric key encryption techniques which use only one key for both encryption and decryption of the data. Their design simple but can be easily cracked using brute force attacks. On the other hand, the second is asymmetric key encryption techniques which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric key encryption ones but lack in time efficiency.

We want to store the data in cloud computing provide many advantages in today's IT world, which enable flexibility and low-cost usage of computing resource. It provides computing resources dynamically via the internet but has some challenges related to data confidentiality, data privacy, and security that may occur. In health care industries record are extremely sensitive; therefore required more security and privacy when storing and sharing those records. The security, as well as the privacy of the sensitive health records, is the major challenge that prevents in the health care industries. To prevent this from unauthorized Access to the health records the user will have to be authenticated to get access to the record. In this paper, we have developed a new health care system to increase patient trust and information integrity through privacy and security. By using the ECC with CP-ABE are providing more security and privacy of health care records. the implementation is proposed using python as the high-level programming language. python supports built libraries to develop cryptographic implementations. There are many third-party organizations and developer communities that provide cryptographic extensions to develop projects. Minimum time required to access and deliver records. To make the system more secure. Less time spent on non-value-added tasks.

II. AIM & OBJECTIVE

The purpose is to design a medical application that contains up to date information about the medical industry. That should improve the efficiency of medical record management. Providing the online interface for data owner and data user etc. Increasing the efficiency of medical record management. Minimum time required to access and deliver user records. To make the system more secure. Less time spent on non-value-added tasks.ECC is better than RSA, they provide better security by our proposed system. The CP-ABE are providing more security and privacy of health care records. The main aim of the proposed system to increase patient trust and information integrity through privacy and security.

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

III. LITERATURE SURVEY

Yujiao Song, HaoWang, XiaochaoWei, LeiWu: They design an ABE scheme that protects user's privacy during key issuing. In this scheme, they separate the functionality of attribute auditing and key generating to make ensure that the KGC cannot know the user's attributes and so that the attribute auditing center (AAC) cannot obtain the user's secret key and the date will be secure.

Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood_, and AtaUllah Ghafoor: In this paper Storing sensitive data on untrusted servers is a big challenge. For confidentiality, proper access control for sensitive data and encryption techniques are used. However, such access control strategies are not feasible in cloud computing because of their insufficiency of flexibility, scalability, and fine-grained access control.

Rather then that Attribute-Based Encryption (ABE) techniques are used in the cloud. This paper completely surveys all ABE schemes and creates a balancing table for the key criteria in cloud applications.

Kamlesh Gupta; Sanjay Silakari; Ranu Gupta; Suhel A. Khan: They are proposed an image encryption method using elliptic curve cryptography (ECC).

RSA is too slow than ECC because ECC requires a smaller key size. In this technique, every pixel of the original image is transformed into the elliptic curve point (Xm, Ym) and those elliptic curve points convert into cipher image pixel. The proposed system gives an equally small block size, high speed, and security.

Saeid Bakhtiari; Subariah Ibrahim; Mazleena Salleh; Majid Bakhtiari: They are proposed image encryption by using ECC and before image compression is proposed system. The results of the proposed system and analysis of applying ECC for image encryption/decryption, encryption performance, and compression performance.

M. Vignesh, Naresh: In Electronic Health Records data stored on the cloud they need security and privacy concerns. Different technic was proposed to prevent both internal and external threats in the healthcare structure. In this paper, different access control mechanisms are used to gives security and confidentiality on Personal Health Records. Electronic Health Record, Cloud data Storage, Access Control mechanism ...etc

Karishma Bhirud, Dipashree Kulkarni, Renuka Pawar, Prachi Patil: Their proposed system used an Elliptic Curve Cryptography algorithm.

The ECC has generated the key using a point on the curve and encryption and decryption techniques happen through the curve. In this paper, the encryption and key generation process takes place rapidly.

Vipul Goyal, Omkant Pandey, Amit Sahai Brent Waters x: In this paper, they develop a new cryptosystem to grain and shared encrypted data that is known as Key-Policy Attribute-Based Encryption (KP-ABE). The ciphertexts are tagged with sets of attributes and the private keys are connected with access structures that control which ciphertext user can decrypt the data. They show the applicability of construction to the sharing control list and broadcast encryption. The construction supports the delegation of private keys which carry a Hierarchical Identity-Based Encryption (HIBE).

IV. PROPOSED SYSTEM

To avoid the drawback of the existing manual system, we propose the computerized system. This system helps in maintaining the database of the medical organization. This system provides easy access to patient information at any time and can be kept safely for a long period without any damage.

A manual system requires a lot of time and manpower. But, in this system, all work is computerized. So, the accuracy of the data is also maintained. Maintaining backup is very easy also. This system allows authorized members to access the record of the medical industry. date owner will manage the whole system.

The design of the patient healthcare information management system. we propose a novel updated CP-ABE system which can be used for the medical record. we develop medical healthcare application where data owner will be select the file from their system and generate public and private key's by using ECC algorithm, While date owner defines the access policy by using CP-ABE and encrypt a file by using AES (128 bit) algorithm will be stored in personal system Data user will send a request to the data owner for accessing records.

If the requested record is found the key will be exchanged using the Diffie-hellman key exchange algorithm. while checking access policy in the ciphertext of the attribute-based decryption can be done or else due to unauthorized accesses and noncompliance of the access policies decryption will be denied.

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

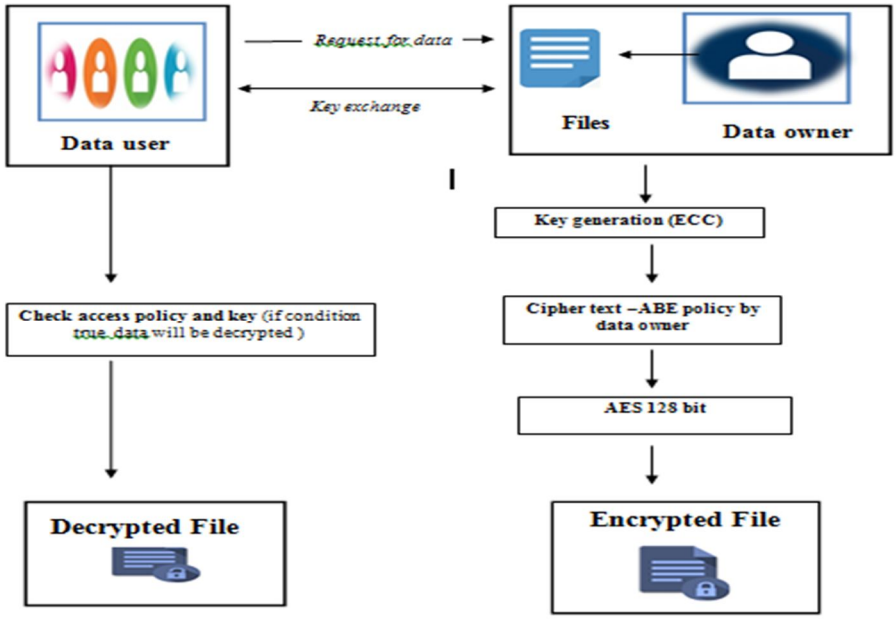


Fig: system flow Diagram

A. Modules

1) *Data Owner:* The data owner will select the file from their system and will generate public and private keys by using the ECC algorithm, while the data owner defines the access policy by using CP-ABE(ciphertext attributed based encryption) then encrypts the file by using AES (128 bit) algorithm. The encrypted file will be stored on the personal system.
2) *Key Generation:* The public and private keys will be generated By using the ECC algorithm.
Using the form y2=x3+ax+b.
3) *Ciphertext –ABE policy:* The data owner will decide the access policy for authorized users, who will have decryption access for the encrypted files.
4) *Encrypted File:* The data owner will encrypt the data file using CP-ABE and AES(128 bit)algorithm.
5) *Decrypted File:* Data user request for a file to the data owner. The key will be exchanged using the Diffie –Hellman key exchange algorithm. The data owner will check the key with CP-ABE access policy with keys, if the accesses policy condition is satisfied then decryption will be performed otherwise decryption is not allowed to the data user.
6) *Data User:* The data user will send a request to the data owner for accessing records. if the requested record is found the key will be exchanged using the Diffie-hellman key exchange algorithm. while checking access policy in the ciphertext of the attribute-based decryption can be done or else due to unauthorized accesses and noncompliance of the access policies decryption will be denied.

V. RESEARCH METHODOLOGY

A. Elliptic Curve Cryptography

Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security. Elliptic curves are applicable for key agreement, digital signatures, pseudorandom generators, and other tasks. Indirectly, they can be used for encryption by combining the key agreement with an asymmetric encryption scheme. They are also used in several integer factorization algorithms based on elliptic curves that have applications in cryptography, such as Lenstra elliptic curve factorization.

The use of elliptic curves in public-key cryptography was proposed by Koblitz and Miller independently in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography.

A general elliptic curve takes the general form as:

y2=x3+ax+b

Where x, y are keys and a, b are integer modulo p, which satisfies

B. Diffie-Hellman Key Exchange

Diffie -Hellman key exchange Algorithms is developed by Whitefield Diffie and Martin Hellman in 1976 to overcome the problem of key agreement and exchange. It enables the two parties who want to communicate with each other to agree on a symmetric key, the key can be used for encrypting and decryption, note that Diffie Hellman key exchange algorithm can be used for only key exchange not for encryption and decryption process. The algorithm is based on mathematical principles.

The algorithm is based on Elliptic Curve Cryptography which is a method of doing public-key cryptography based on the algebra structure of elliptic curves over finite fields. The DH also uses the trapdoor function just like many other ways to do public-key cryptography.

A general form as:

$(g^a \ mod \ p)^b \ mod \ p = g^{ab} \ mod \ p$

$(g^b \ mod \ p)^a \ mod \ p = g^{ba} \ mod \ p$

C. Attribute-Based Encryption

It is a public key algorithm based on many encryptions and user attributes that allows the users to encrypt and decrypt the information so that the structured accessed contains the certified sets of attributes and restricts the notice to monotone access structure.

1) Attribute-based encryption is more flexible.

2) The ABE is secure because the encryption data contain the attributed rather than data

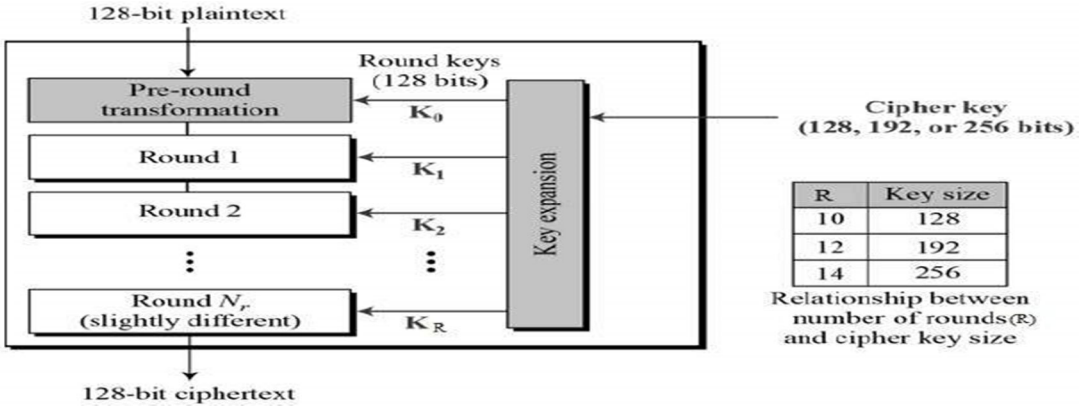
a) *Key Policy ABE:* In KP ABE data sender use a collection of attributes to labels cipher. A trusted authority issues the private key of the user from an access structure that specifies the type of ciphertext that can be decrypted. The KP ABE is suitable for organizations with hierarchies that specify which file is accessible by which user.

b) *Cipher-Text Policy ABE:* In CP-ABE Scheme a data sender encrypts the message using a traditional encryption scheme. An access policy is specified in form of access structure over attributes in the cipher-text. The access structure specifies users that are capable of accessing the cipher-text. The users decrypt the cipher-text if only their attributes match the access policy associated with the encrypted data.

- It is more suitable for use in actual Applications within the environments.
- It is capable of specifying the users that can decrypt the encrypted version of the file.

D. AES Algorithm

AES is an iterative rather than a Feistel cipher. It is based on 'substitution–permutation network'. It comprises a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. The schematic of the AES structure is given in the following illustration



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Fig. schematic structure of AES

VI. CONCLUSION

Health Care System lead to a better organization structure since the information management of the patients is well structured & also lead to better as well as efficient utilization of resources. The system has been developed error free and at the same time, it is efficient and less time-consuming.

This system is only for the health care industries. The information is stored in the system can be accessed at any time by using this system & there will be no wastage of resources in health care industries. So this system performs paperless work & manages all data efficiently. It provides easy, accurate, unambiguous & faster data access.

The purpose of developing this software is to generate the desired reports accesses as required. We Conclude that this project adequately manages all the information & provide security to the medical record.

REFERENCES

[1] Muhammad Yasir Shabir, Asif Iqbal, Zahid Mahmood_, and AtaUllah Ghafoor, Analysis of Classical Encryption Techniques in Cloud Computing, TSINGHUA SCIENCE AND TECHNOLOGY, Volume 21, Number 1, February 2016

[2] Yujiao Song,1 HaoWang,1,2 XiaochaoWei,1 and LeiWu 1,3 Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud, Hindawi Security and Communication Networks Volume 2019, Article ID 3249726

[3] Manish Kumar1, Rachid Ait Maalem Lahcen3, R. N. Mohapatra3, Chandan Alwala2, and Surya Vamsi Krishna Kurella2 *Jan - Feb 2020*, Review of Image Encryption Technique.

[4] Nirbhay Sibal, Tanvi Hasija, Shally Gupta, ICCCS - 2017 Conference Proceedings, Secure Transmission of Data by Elliptic Curve Cryptography.

[5] John Bethencourt, Amit Sahai, and Brent Waters, Ciphertext-Policy Attribute-Based Encryption US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316

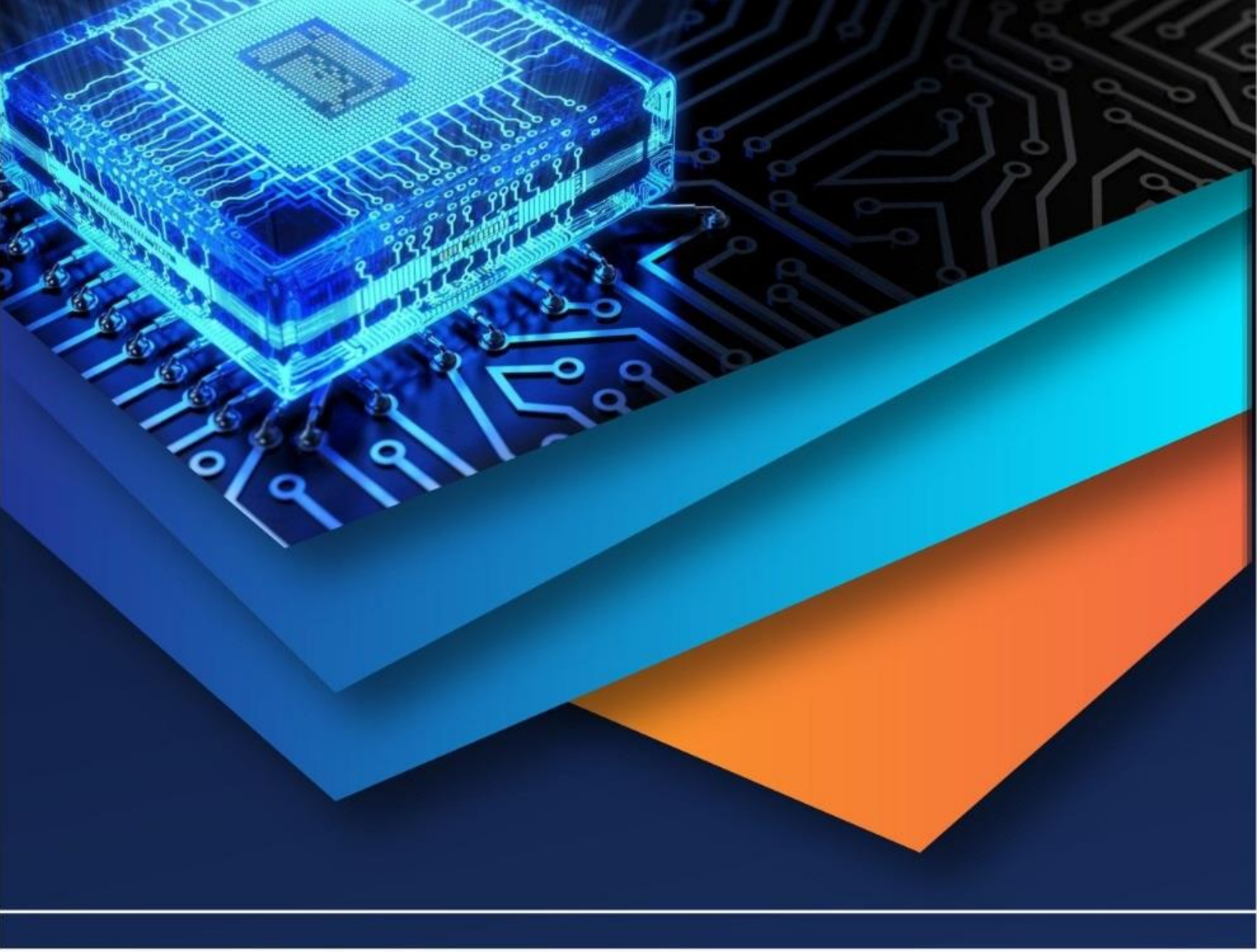
[6] Rahul Singh, Ritu Chauhan, Vinit Kumar Gunjan, Pooja Singh, Implementation of Elliptic Curve Cryptography for Audio Based Application International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 1, January - 2014 IJERTIJERT ISSN: 2278-0181

[7] Mohan Kumar M and Vijayan R, Privacy authentication using key attribute-based encryption in mobile cloud computing, IOP Conf. Series: Materials Science and Engineering, 14th ICSET-2017

[8] K. Shankar and 2Dr. P. Eswaran, ECC Based Image Encryption Scheme with aid of Optimization Technique using Differential Evolution Algorithm, International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.55 (2015).

[9] Satish T. Pokharkar, Manoj Kumar Rawat, Multi-Authority Secure Database for Enabling Authorized Encrypted Search with Privacy-Preserving on Healthcare Databases, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-9 Issue-1, May 2020.

[10] Suseela g, a snath victory family y, low bitrate hybrid secured image compression for wireless image sensor network, advances in smart computing and bioinformatics, 23 January 2017, revised and accepted: 03 March 2017



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY