International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhanced Blowfish Algorithm and EECC to Improve Cloud Storage Security

Thotakuri Srilekha[1], Vijay Bhanu S.*[2], Niranjan P.[3]

Submitted: 08/05/2023 **Revised**: 18/07/2023 **Accepted**: 09/08/2023

Abstract: Several applications consist of huge volume of data associated to its function. Data handling is the major concern in all application which relies in internet, Cloud is feasible solution to store such data used in internet applications but the security is a big concern and its privacy, security parameters are also degraded when these data are placed in common private storage place. Generally numerous techniques of cryptography are being involved in securing those third party storage places but still it is integrity questionable. We have proposed a method named EBF-EECC (Enhanced Blowfish Algorithm –Enhanced Elliptic Curve Cryptography) for securing data as well as key. Key is encrypted separately by EECC and Data encrypted separately with the help of EBF. In addition with these techniques we deployed one more hash function along with EBF-EECC for concrete safety of the data pertaining to individual services in the cloud. Blowfish algorithm is still being used for securing the data in excellent manner with the help of Average size of the key, Number of rounds and the sizes of block and the same proved in our simulation. Elliptic curve cryptography is also considered in proposed method by taking their strong nature of key sizes considered with other algorithms like RSA to improve concrete security measurement on cloud data.

Keywords: *Cloud storage, Data Encryption, Data Privacy, Data Security, Encryption Key*

1. Introduction

Integrity, Availability, and access are the three major hindrances in cloud registering. The major deterrent in the cloud is availability. At the point when illicit admittance to data is acquired, the ability to change customer information arises. Also, accessibility is a hindrance where information should be accessible consistently for customers without concerns influencing capacity and bringing about information misfortune in the cloud. One more hindrance in the cloud is respectability, which is utilized to fix information and in the security field to control or shield information on the cloud, with the significant spotlight on the specialist organization [1].

There are an assortment of safety concerns and issues related with distributed computing, however they can be isolated into two classifications: security issues looked by cloud suppliers associations that give foundation as an assistance , stage as a help , or programming as an assistance through the cloud and security issues looked by their clients. Much of the time, the supplier is answerable for guaranteeing that their framework is protected and that their customers' information and applications are secured, while the client is liable for guaranteeing that the supplier has taken the fundamental security safety measures to ensure their information [2].

1.1 Data Security in cloud

Cloud processing is a generally new improvement in the realm of systems administration and software engineering. It has made roads for little and medium-sized organizations to accomplish their objectives without squandering cash on equipment buys. It furnishes everybody with an equivalent chance to sparkle. Cloud registering is based on the virtualization thought, in which a solitary enormous machine is shared by various clients, every one of whom has their own devoted assets [3].

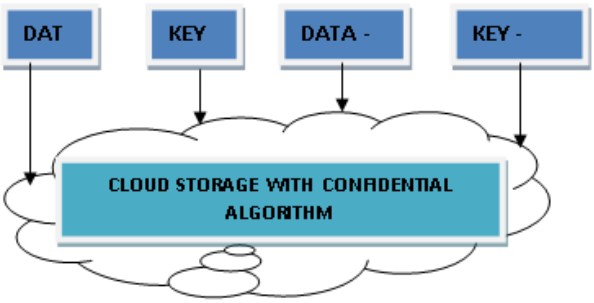

Fig 1: Secure Cloud Data

The data stored in third party place is an idle solution rather than maintaining separate resources to store in our own firm. But manipulation on those data is not that much guarantee when it is being kept in others place. Essential mechanism is needed to safeguard the information retained in the cloud. Encryption is one of the major defender to safeguard the relevant data in the cloud which ensures integrity of the data.

[1]*Research Scholar, Dept. of Computer Science & Engg., Annamalai Univ*
[2]*Research Supervisor,Dept. of ComputerScience&Engg., Annamalai Univ*
[3]*Research Co-Supervisor, Dept. of CSE., Annamalai University*
** Corresponding Author Email: svbhanu22@gmail.com*

Elliptic curve cryptography is focusing on key encryption and blow fish algorithm is concentrate on data as well as key encryption. Blowfish algorithm and Elliptic curve cryptography algorithm extended with a hash function which applied to the output of both algorithms to generate hash value to provide addition security measurement to the data stored in third party cloud stores. The Figure 1 shows the steps of extended EBF and EECC concepts.

2. Related Works

While putting away private or privileged information on the cloud, information secrecy is basic. To guarantee information secrecy, confirmation and access control instruments are utilized. Cloud registering difficulties like information classification, confirmation, and access control could be settled by further developing cloud dependability and reliability. One of the main parts of any data framework is information honesty. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Dealing with an element's admittance to specific venture assets guarantees that touchy information and administrations are not abused [4-5].

Data Privacy is about a person's or a gathering's capacity to segregate themselves or data about themselves and specifically uncover them is known as protection. Coming up next are the parts of security. It's conceivable that a subject is more restless with regards to current or future data being uncovered than earlier data. A client might be calm if their companions can physically demand their data, yet the person may not see the value in programmed and successive updates. Rather than a particular point, a client's data might be accounted for as an equivocal zone [6].

2.1 Contribution of Security Algorithms

Blowfish and other symmetric-key based calculations require moving the private key, which can be dangerous because aggressors may steal the key. To obtain the private key and hash code in this configuration, we use an elliptic-bend based uneven cryptography calculation. A 164-cycle key will be used in this method to provide a better presentation than other options. In Fp, there are six choices for adding two unique focuses to the elliptic bend: one square, two increases, and one converse activity. On the elliptic bent, point multiplying requires eight augmentations, two squares, two duplications, and one opposing activity. We begin by selecting an elliptic bent algorithm for cryptography [7-8].

The significance of data security couldn't possibly be more significant. Cloud registering is a strategy for accessing figuring and data assets from any area with an organization. There is an interest to shield information put away in the cloud. The encryption calculation's essential objective should be to ensure against uncertified attacks. Nonetheless, valuing and execution are significant difficulties for all cloud figuring applications. If an encryption calculation is defensive yet sluggish to perform, it is of little use. Encryption calculations should be equivalent as far as execution and security [9].

3. Methodology

The protection safeguarding public inspecting instrument was utilized, just as an outsider free element inspector. The exploration's significant objective was to refresh the data or to work on the data's respectability and audit ability. This review included encryption procedures like Secure Hash Algorithms and the Advanced Encryption Standard plot, just as the idea of reduplication or giving server access privileges. The review's significant objective was to find copy information and cut down on data transmission use [10].

Blowfish encryption and Homographic encryption techniques are utilized to get the cloud. Since homographic encryption depends on bits, this review takes a number N, changes it over to twofold, and afterward utilizes homographic encryption to scramble every one of its pieces. At last, these strings are connected and communicated to the second layer of the blowfish technique. Decryption follows the indistinguishable strategies as encryption, yet it accepts the scrambled message as information, applies it to the blowfish decryption layer, and afterward yields the decoded message [11].

Blowfish is a symmetric block cipher encryption calculation, which implies it encodes and unscrambles messages utilizing similar mystery key and partitions them into fixed-length blocks during encryption and decoding. Blowfish has a 64-cycle block length, so messages that aren't products of eight bytes should be cushioned. It utilizes a variable-length key going from 32 to 448 pieces, making it ideal for information security. It's great for applications like an interchanges interface or a programmed document encryption where the key doesn't change oftentimes. At the point when executed on 32-cycle microchips with enormous information reserves, it is significantly faster than other encryption procedures [12].

A blend of RSA and BLOWFISH is utilized in this half breed security instrument. The choice to consider such a blend was predicated on the way that blowfish is both compelling and unpatented, making the cryptosystem financially savvy, and RSA, which is practically normally utilized for advanced marks. In the wake of verifying into the code cloud, the proposed method can be utilized for cloud processing on a FPGA organization. The information of decision is then moved to the cloud server, which

decodes the solicitation utilizing a symmetric key given by the server and afterward encodes it with RSA [13-14].

The consolidate eradication codes over types with a recently proposed limit intermediary re-encryption method. The limit intermediary re encryption framework considers dispersed encoding, sending, and fractional unscrambling. In our framework, each key server just requirements to some extent decode two codeword images to unscramble a message of k squares that are scrambled and encoded to n codeword images. We portray a protected cloud stockpiling framework that gives safe information stockpiling and secure information sending usefulness in a decentralized construction using the edge intermediary re-encryption calculation. Moreover, every capacity server does encoding and re-encryption all alone, as does each key server [15-16].

Elliptic Curve Cryptography (ECC) is a procedure for planning public key cryptography conventions, for example, executing keys and computerized marks. There are an assortment of impetuses for utilizing elliptic curves, including the way that they give all the more little key sizes and execution choices. ECC is an open cryptosystem like RSA. Notwithstanding, its quicker pace of headway, just as the way that it offers a really engaging and adaptable strategy to cryptographic working out specialists, makes it stand apart from RSA. ECC can give a comparative degree of safety to that given by RSA, yet with more modest key sizes [17-18].

Both the private and public keys are created utilizing ECC, a public-key cryptosystem. ECC will make two keys for every client, the first is alluded to as the private key and the second as the public key. Client A utilizations User B's public key to encode the plain message and sends the code message to the cloud. Client B can get to the code text from the cloud whenever. Client B then, at that point, decodes the code message with his own private key to get the plain message that User A sent. The sent information can't be seen by others since the private key is kept mystery. Coming, information in the cloud will be safer [19-20].

4. Implementation

The focus of our development is securing the data in cloud usually the encryption will be done with the help of Key and Encryption then send together in medium to dispatch the same at receiving side .The process development is specified in below flowchart Figure 2. The process starts with performing key encryption for the data stored in cloud. Encryption using EBF and EECC is applied to whenever the data stored and retrieved in the cloud. The algorithm is available in cloud to perform encryption whenever the data is being accessed by client whoever associated with this .Initially key value consider for encryption and then data is also considered as separate encryption process which is then send to hash function to check the data is manipulated during transmission between client and cloud store.

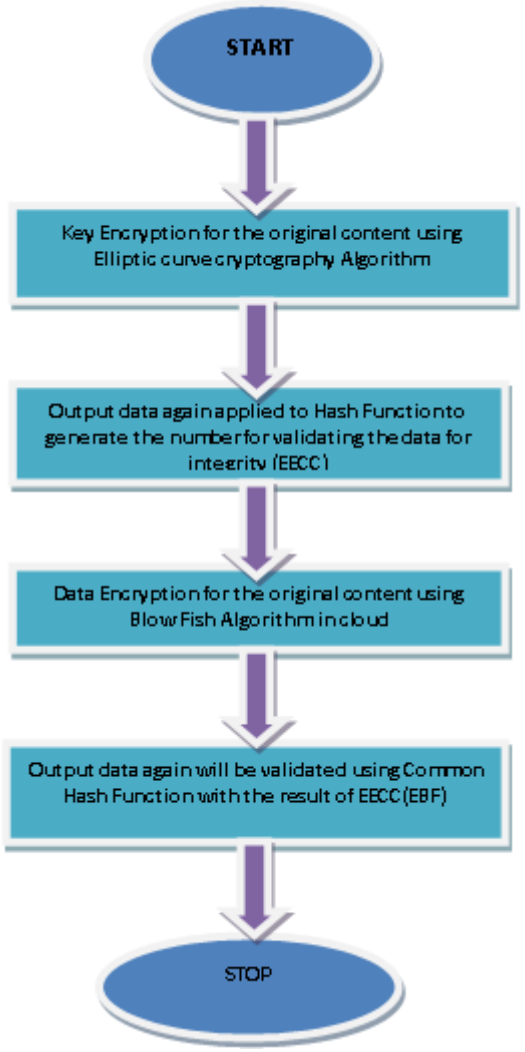

Fig 2: Flowchart for EBF and EECC

4.1 Enhanced Blowfish algorithm for cloud security:

Cryptographic algorithms are a set of technologies and equations that enforce security on data and networks. Cryptography is the science of determining the most effective methods for transferring information in a secure manner, with only the intended recipient having access to the message. Encryption is critical in communication because it prevents unauthorized people from reading the message .The decryption process is the process of turning encrypted text to plaintext.

The Blowfish algorithm was made by Bruce Schneier as a symmetric-key square code. The tangled key booking and key-subordinate replacement boxes are two of the calculation's most outstanding elements. The procedure utilizes a 64-bit block size and a key size that reaches from 32 to 448 pieces. The P-exhibit and the four Sboxes make up a 16-round Feistel Cipher with sub key clusters. The

Blowfish calculation has four stages in each round. The left half of the square is XORed with the nth P-exhibit in the nth round, then, at that point, passed into the Blowfish calculation's F work. The F capacity's result is XORed with the right 50% of the first square prior to being traded [21-23].

Asymmetric Key Algorithm, frequently known as open key cryptography, is a kind of unbalanced key calculation. 'Private Key' and 'Public Key' are the two keys utilized. Preceding transmission, the sender encodes the plain message with the assistance of the public key to make figure message, which the collector unscrambles with the assistance of its private key. By raising the document size and key length, the blowfish calculation's exhibition improves. The Blowfish Algorithm is likewise utilized in the Password Management System. In the Clipper and Capstone chips, the procedure has likewise been utilized in bitmap picture plotting instead of mystery calculations like the Skipjack calculation. Execution was likewise evaluated by changing its capacity, which yielded positive discoveries that were depicted [24-26].

Blowfish's key timetable is extended, comparable to scrambling 4KBs of information, which may be a block or an advantage. On the negative side, it consumes most of the day to finish. Due to Blowfish's small square size, Birthday Attacks can happen, compromising the encryption method. It's trailed by Twofish, which was intended to supplant Blowfish and is predominant in pretty much every respect. Each encryption method has its own set of strengths and weaknesses. In order to apply a suitable cryptography algorithm to an application, we must first understand the algorithms' performance, strengths, and weaknesses. As a result, these algorithms must be evaluated using a variety of criteria. In this work, the cryptosystems are analyzed using the following measures to compare them: Time to encrypt, time to decrypt, avalanche effect, memory used [27-28].

4.2 Comparison of EBF with other algorithms

Encryption time is the time it takes for an encryption algorithm to transform plaintext data to cipher text. It's a measure of the algorithm's effectiveness. The encryption time is measured in milliseconds in the following analysis, and it is regarded a factor in assessing the speed of encryption in networks.

Decryption time is the time it takes an encryption algorithm to convert ciphertext data to plaintext data. The algorithm's efficiency increases as the decryption speed decreases. The decryption time is measured in milliseconds in the following study, and it is also used to determine the wireless network's speed. A cryptosystem's throughput is measured in gigabytes of plaintext encrypted every millisecond by the algorithm. A system with a higher throughput is one that is more efficient. Mbps is the measuring unit [29-30].

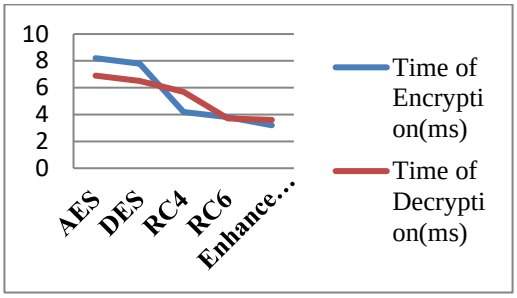

Fig 3: Encryption time and Decryption time of various algorithms

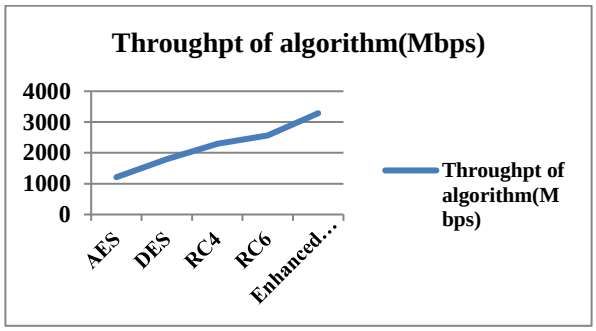

Fig 4: Throughput comparison of EBF with other algorithms

Before comparing the enhanced EBF with hash implementation of its, we have implemented and verified the comparison of various algorithm with blowfish algorithm in terms of association with its ability of less encryption and decryption time. Throughput of each algorithm also considered and tested in our proposed techniques of enhancing with the support of hash value. The Figure 3 x axis depicted by naming of algorithms used in our simulation, on the other hand y axis represented in millisecond unit of both encrypt and decrypt time. Figure 4 x axis as considered in figure 3 x axis parameter and y axis represented with Mbps. The normal encryption is applied to both key and data together with a common algorithm. Here we have separated and applied encryption for data and key [31][32].

The above comparison made from the result of our simulation and represented. Here simulation performed as one module in which we have observed the value of blowfish algorithm for our sample application and collected date. Then the same data set is applied with EBF module which is the combination of Hash function and blows fish algorithm concepts. The performance of extended ECC is improved percentage when compare to normal ECC. BlowFish algorithm is still providing excellent security when compare to other cryptographic algorithm with its own unique and moderate level of its key size, block size[33].

DEncrpt = Key + Data → Equation 1

DDecrpty= Key + Data → Equation 2

Process = Equation 1 + Equation 2

In EBF + EECC

EBFDEncrypt = Key + Data + Hash → Equation 3

EBFDDecrypt = Key + Data + Hash → Equation 4

EECCDEncrypt = Key + Hash → Equation 5

EECCDDecrypt = Key + Hash→ Equation 6

Process in EECC = Equation 5 + Equation 6 → Equation 7

Process in EEBF = Equation 3 + Equation 4 → Equation 8

Overall Process = Equation 7 + Equation 8

The above steps explained are the process of encryption and decryption process of our methodology where it is deployed in the cloud for securing the data in the cloud. We have simulated the entire proposed concept with the help of python tool because it has all models of cryptographic algorithm in its package.

The outcome of the ECC further applicable to process of hash function to maintain originality check of the data stored in cloud. Here one parameter represented by methods and another attributes are represented by percentage of result in further section. Finally we have compared the overall performance of the extended encryption process in terms of Hash and it is named as EBF and EECC. The outcome shows that gradual increment in performance observed in our implementation. But the complex is little overhead in other parameter specifically memory overhead in execution.

5. Conclusion

At the point when we store information on the cloud, we should be worried about security since it is vigorously dependent on a web association. Information put away in an outsider area is helpless against interruption by interior or outer people whenever. Encryption is one of the choices accessible for information security. To communicate information in another structure, an assortment of strategies, for example, rendering and substitution methods are as of now open. Be that as it may, programmers who are endeavoring to break the security region can utilize these ways to deal with do as such whenever. Lopsided and symmetric encryption is currently being utilized to ensure information put away in the cloud against security breaks. Subsequently, it requires a strong system that consolidates more than one existing plan and can't be broken once more.

Acknowledgements

This research was not funded & supported.

Author contributions

Srilekha – Developed full article, Vijaybhanu – guided & reviewed full article, Niranjan – Reviewed.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Tannu, Karambir (2017) Enhancing data security in cloud using encryption techniques. Indian J Comput Sci Eng 8(3):280–283

[2] Prabhu et.al., “Privacy preserving steganography based biometric authentication system for cloud computing environment”, Measurement: Sensors Journal, Vol 24, Dec 2022, https://doi.org/10.1016/j.measen.2022.100511

[3] Handa K, Singh U (2015) Data security in cloud computing using encryption and steganography. Int J Comput Sci Mob Comput 4(5):786–791

[4] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, andGuangyu Zhu, Data Security and Privacy in Cloud Computing, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903

[5] Pon H, et.al., “Conceptual approach on smart car parking system for industry 4.0 internet of things assisted networks”, in Measurement: Sensors, Volume 24, December 2022, https://doi.org/10.1016/j.measen.2022.100474

[6] J. Krumm, “A survey of computational location privacy,” Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399, 2009.

[7] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, "A comparative survey of symmetric and asymmetric key cryptography," in 2014 international conference on electronics, communication and computational engineering (ICECCE), 2014: IEEE, pp. 83-93.

[8] Hossein Abroshan, A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 6, 2021

[9] Neha MK (2016) Enhanced security using hybrid encryption algorithm. Int J Innov Res Comput Commun Eng 4(7):13001–13007

[10] Salem MZ, Sabbeh SF, EL-Shishtawy T (2017) An efficient privacy preserving public auditing

mechanism for secure cloud storage. Int J Appl Eng Res 12(6):1093–1101

[11] Sajay, K.R., Babu, S.S. Enhancing the security of cloud data using hybrid encryption algorithm. J Ambient Intell Human Comput (2019). https://doi.org/10.1007/s12652-019-01403-1

[12] Sumalatha Potteti, Namita Parati, Secured Data Transfer For Cloud Using Blowfish, International Journal of Advances In Computer Science and Cloud Computing, Volume- 3, Issue- 2, Nov-2015

[13] C. Curino, E. Jones, P. C., Popa, R. A., Wu & N. Zeldovich, "Relational Cloud : A Database-as-a-Service for the Cloud Accessed Citable Link Relational Cloud : A Database-as-a-Service for the Cloud," Information Applications, vol. 1, no. 1, 2011, pp. 0–6.

[14] Shafi'i Muhammad Abdulhamid, Nafisat Abubakar Sadiq, Mohammed Abdullahi, Nadim Rana3, Haruna Chiroma, and Dada Emmanuel Gbenga, Development of Blowfish Encryption Scheme for Secure Data Storage in Public and Commercial Cloud Computing Environment, 2nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018) Federal University of Technology, Minna, Nigeria September 5 – 6, 2018

[15] Abdullah Th Abdalsatir, Mohammed Farooq Hamdi, Ali Noori Kareem, Data Security in Cloud by Using Blowfish Algorithm, International journal of scientific and Technology research ,ISSN 2319-8885 Vol.03,Issue.01, Pages:0158-0162, January-2014

[16] B. Umapathy and D. Kalpana, "A Survey on Cryptographic Algorithm for Data Security in Cloud Storage Environment," European Journal of Molecular & Clinical Medicine, vol. 7, no. 09, 2020.

[17] Thyagarajan C, et.al., "A Typical Analysis and Survey on Healthcare Cyber Security" in Int. Journal of Scientific and Technology Research, Vol.9, Issue.3, pp.3267-3270, 2020, ISSN: 2277-8616

[18] Vijayalakshmi C, Florence, "A survey on solving dilemmas of adapting blockchain in different applications" 1st International Conference on Recent Advances in Manufacturing Engineering Research, ICRAMER 2021, AIP Conference Proceedings, 2460, 070011 (2022); https://doi.org/10.1063/5.0095701

[19] Nivethitha Vijayaraj,Sivasubramanian Arunagiri, "Intensification and Interpretation of Performance in 5G Adopting Millimeter Wave: A Survey and Future Research Direction", The International Arab Journal of Information Technology (IAJIT) ,Volume 20, Number 04, pp. 600 - 608, July 2023, doi: 10.34028/iajit/20/4/6.

[20] Neha Tirthani, and Ganesan R, Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography, International Association for Cryptologic Research Cryptology,49, 2014.

[21] Suthir S & Dr.S.Janakiraman, "Contemporary and efficient shared area network in Peer-to-Peer Communication", International Conference on Radar, Communication and Computing, Proceeding of IEEE XPlore, pp. 38–42, 2012, https://doi.org/10.1109/ICRCC.2012.6450544

[22] Archisman Ghosh . Comparison of Encryption Algorithms: AES, Blowfish and Twofish for Security of Wireless Networks, International Research Journal of Engineering and Technology, Vol:07 Iss:06,2020

[23] Vijayaraj, N., Arunagiri, S. Demultiplexer design using photonic crystal ring resonator with high quality factor and less footprint for DWDM application. Opt Quant Electron 54, 465 (2022). https://doi.org/10.1007/s11082-022-03817-2

[24] Srividya M, et.al., "A contemporary network security technique using smokescreen SSL in huddle network server", 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Proceeding of IEEE XPlore, 2016, pp 673-676, https://doi.org/10.1109/AEEICB.2016.7538376

[25] Nivethitha.V, M.Bhavithra – "Real Time Sectionalization of Enhanced Sharpness Video using FPGA" in Elysium Journal of Engineering Research and Management, Volume 3, Issue 4, Page No. 23 - 26, August-2016. ISSN: 2347-4408.

[26] Wafaa A. N. A. AL-Nbhany, Ammar Zahary, A Comparative Study among Cryptographic Algorithms: Blowfish, AES and RSA, International Arab Conference on Information Technology.

[27] Suthir S and Janakiraman S, "SNT Algorithm and DCS Protocols coalesced a Contemporary Hasty File Sharing with Network Coding Influence", Journal of Engineering Research, Vol. 6, Issue 3, pp.54-69, 2018

[28] Jayashri C, et.al., "Big Data Transfers through Dynamic and Load Balanced Flow on Cloud Networks", 3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics, AEEICB 2017, Proceeding of IEEE XPlore, pp. 342–346, 2017, https://doi.org/10.1109/AEEICB.2016.7538376.

[29] Dr.S.Janakiraman, et.al., May-2017. "A Survey of Fast File Sharing System in Network" in International Journal of Engineering Development and Research, Vol. 5, Issue: 2, May 2017, pp. 1298-1304, ISSN: 2321-9939, https://zenodo.org/record/583721

[30] Taha Junaid, et.al., "A comparative analysis of transformer based models for figurative language classification", Computers and Electrical Engineering, vol. 101, July 2022, https://doi.org/10.1016/j.compeleceng.2022.108051

[31] Krishnamurthy A, Kumar B," The Repaschine: A Robot to Analyze and Repair Roads Using Cutting-Edge Technologies, EAI/Springer Innovations in Communication and Computing, pp. 249–254, 2021, https://doi.org/10.1007/978-3-030-49795-8_24

[32] Prabhu D, et.al., "Design of Multiple Share Creation with Optimal Signcryption based Secure Biometric Authentication System for Cloud Environment",International Journal of Computers and Applns., 2022, 44(11), pp. 1047–1055, https://doi.org/10.1080/1206212X.2022.2103890

[33] Elumalaivasan et.al.," CBIR- Retreival of Images using Median Vector Algorithm", International Conference on Green Computing, Communication and Conservation of Energy, ICGCE 2013, Proceeding of IEEE XPlore, pp. 1–5, 2013, https://doi.org/10.1109/ICGCE.2013.6823389

[34] Singh, S. ., Bharti, A. K. ., Pandey, H. ., Yadav, R. K. Sharma, D. ., & Shanker, N. (2023). Towards Automated and Optimized Security Orchestration in Cloud SLA. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 215–222. https://doi.org/10.17762/ijritcc.v11i3.6339

[35] Chaudhary, D. S. ., & Sivakumar, D. S. A. . (2022). Detection Of Postpartum Hemorrhaged Using Fuzzy Deep Learning Architecture . Research Journal of Computer Systems and Engineering, 3(1), 29–34. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/38

[36] Soundararajan, R., Stanislaus, P.M., Ramasamy, S.G., Dhabliya, D., Deshpande, V., Sehar, S., Bavirisetti, D. P. Multi-Channel Assessment Policies for Energy-Efficient Data Transmission in Wireless Underground Sensor Networks (2023) Energies, 16 (5), art. no. 2285,