# A Methodology For Secure Sharing Of File Records In The Cloud

Modagala Hari Prasad [1], Dr.T.V.S Gowtham Prasad [2]
P.G. Student, Department of Electronics and Communication Engineering, Sree Vidyaniketan Engineering College, Sainath .Nagar ,Tirupati, Andhra Pradesh, India[1]
Associate Professor, Department of Electronics and Communication Engineering, Sree Vidyaniketan Engineering College, Sainath Nagar , Tirupati, Andhra Pradesh, India [2]

*Abstract:* Secure chase over combined a long way away measurements is primary in disseminated processing to assure the facts coverage and straightforwardness of utilization. To thwart unapproved actualities use, great-grained get admission to govern is crucial in multi-customer structure. Be that as it could, accepted purchaser may furthermore intentionally dispatch the spine chiller key for money associated gain. Along those strains, following and repudiating the vindictive customer who abuses backbone chiller key ought to be understood short. Execution examination with appreciate to time utilization indicates that the gadget would possibly be capable of use for undauntedly sharing the inside the cloud. Conjointly we are able to in popular Implement as a willpower at a few segment on this paper time Server, Secure Auditing Storage, in Time Server Owner include the begin and Ending time be a part of two moved Encrypted records. In this, we suggest an escrow loose perceptible characteristic fundamentally primarily based various catchphrases subset search shape with verifiable redistributed unscrambling. The key escrow free framework must as it should be avoid the important thing age attention from misleadingly searching and disentangling all blended facts of clients. Moreover, the unscrambling framework just requires especially lightweight computation, which is an attractive element for energy compelled devices. Moreover, effective customer repudiation is enabled after the threatening purchaser is made involvement.

**IndexTerms**: Access control, cloud computing, privacy, Secure Auditing Storage.

## I. INTRODUCTION

Cloud computing is the on-demand availability of PC device property, basically data collecting and figuring vitality, without direct effective organization with the manual of the purchaser. The term is usually used to depict server cultivates available to three customers over the Internet. Gigantic fogs, otherworldly today, frequently have limits handed on various territories from crucial servers. On the off danger that the alliance with the consumer is frequently close, it is maximum probably allotted a server. Fogs can be obliged to a lone alliance, be on hand to three institutions, or a blend of each .Cloud enlisting is predicated upon sharing of advantages for achieve knowledge and economies of scale. With the improvement of ongoing dealing with attitude, disseminated registering turns into the most remarkable one, which gives beneficial, on-call for profits by way of a commonplace pool of configurable figuring resources. Subsequently, an expanding extensive collection of agencies and people want to redistribute their statistics storing to cloud server. Notwithstanding the goliath cash associated and concentrated elements of diversion, sporadic protection and well-being issues become the most apparent hassle that obstructs the irrespective of how you look at it selection of facts storing in open cloud status quo. Encryption is a simple strategy to at ease data assurance in far flung amassing. Regardless, an method to securely execute watchword take a look at for plaintext at ultimate finally ends up difficult for encoded insights in mild of the fresh out of the plastic new restrict of perceive content. Available encryption gives framework to interact watchword search for over encoded records.

For the report sharing gadget, for example, multi-owner multiuser circumstance, excessive quality grained search endorsement is a fascinating potential for the certainties owners to bestow their non-open realities to other authorized client. In any case, the extra noteworthy a piece of the accessible structures require the benefactor to play out a ton of confounded bilinear mixing sports. These overwhelmed counts rise as a big load for client's terminal, this is especially genuine for strength obliged gadgets.

The re-appropriated unscrambling technique enables supporter to get properly the message with extremely-mild-weight interpreting. Be that as it is able to, the cloud server may additionally go back wrong half-unscrambled records due to noxious assault or machine glitch. Thusly, it is a massive problem to make sure the precision of re-appropriated translating in open key encryption with watchword seek machine. Despite the upsides of flexible, agile, monetarily sharp, and unavoidable corporations exhibited thru the cloud, brilliant concerns associated with the safety of prosperity actualities in like way expand. A big motive at the back of sufferers' nerves with renowned to the mystery of is the opportunity of the cloud to share and shop the Storing the character prosperity certainties to cloud servers administered through using untouchables is uncovered to unapproved get to. In precise, protection of the set away in open fogs which might be administered by way of business grasp institutions is very in threat. The security of the can be in risk in a couple of diverse methods, for example theft, catastrophe, and spillage.

The proposed approach moreover continues the forward and in transfer get admission to manage. The aid of past due becoming a member of people from a selected consumer social affair get the keys from the SRS. The shared facts is mixed by means of the keys of the proprietor so to speak. The passageway to the records for as of late becoming a member of part is yielded after the aid of the owner. Basically, a leaving consumer is ousted from the ACL and the relating keys for that customer are eradicated. The deletion of the customer keys and elimination from the ACL achieves repudiation of get right of entry to the for any cockeyed get right of entry to attempts after the customer has pulled returned. Additionally, it's far acknowledged that correspondence between

the purchaser and is confirmed via utilization of standard indicates like, IPSec or SSL. The currently referenced shows are for the most part used over the Internet and are definitely prepared for confirming correspondence. In any case, correspondence protection is beyond the diploma of this paper. The game plan, key age, and re-encryption kills are exceeded on at SRS.

## II.RESEARCH METHODOLOGY

The proposed system is secure as compared to various other constructions used in the sense that the in the proposed framework is never transmitted the data. The proposed scheme employs proxy re-encryption for providing confidentiality and secure sharing of AES through the public cloud. Instead, the responsibility of the is to manage the keys while the ElGamal Encryption Algorithm

Operations are performed by the owners whereas the decryption is performed at the requesting users and having the valid decryption keys.

## III. ALGORITHM

AES Algorithm:
AES (Advanced Encryption Standard) is a symmetric encryption count. It makes use of an equal key for encryption and decoding. A splendid deal of records may be mixed using a symmetric encryption estimation. An essential parameter for AES is the encryption mode. It portrays, how the sport plan of open information squares changed over into encoded onuses key length is 128, 192, 256 bits. The symmetric encryption counts which can be most all around connected are DES, 3DES, AES and RC4. Symmetric encryption is short in execution. The symmetric encryption is hooked up for getting and promoting an all the greater piece of information. As it is completed in every framework and writing laptop programs, it's far high-quality protection display. It makes use of better period key sizes, as an example, 128, 192 and 256 bits for encryption. In this way it makes AES estimation gradually notable toward hacking. It uses too real arithmetical form. Hard to complete with programming application.AES in counter mode is musings boggling to execute in programming taking each execution and safety into mind.

AES followed by Huffman code to reduce Encryption and Decryption time consumptions. It is called as Integrated Encryption System (IES).


**Figure 1**: IES Encryption and Decryption.

Huffman encode is use to covert text to binary form and the also reduce repeated data to single binary form.

Huffam decode will code the original data. It is use for to provide secure to a data.

3.1 El-Gamal Encryption Algorithm:

El-Gamal encryptions an open key cryptosystem. It makes use of unbalanced key encryption for conveying between two gatherings and scrambling the message. This cryptosystem relies upon at the problem of locating discrete logarithm in a cyclic gathering this is regardless of whether or not we recognize and go, its miles very hard to sign up key.

In cryptography, the El-Gamal encryption framework is an uneven key encryption calculation for open key cryptography which depends at the Diffie–Hellman key exchange. El-Gamal encryption is applied within the free GNU Privacy Guard programming, ongoing editions of PGP, and unique cryptosystems. Ought to now not be incorrect for El-Gamal encryption. Proposed the accompanying method to make Diffie-Hellman into an encryption conspire. The El-Gamal Cryptosystem is verifiably based on the hassle of locating a solution for the discrete logarithm in F¤p: given a crude issue an of F¤p and every other component b.El-Gamal encryption can be characterizedover any cyclic amassing, for example, multiplicative accumulating of entire numbers modulo n.

Its protection is based on the hassle of a particular trouble in identified with registering discrete logarithms. Like most open key frameworks, the El-Gamal cryptosystem is generally utilized as a chief factor of a crossover cryptosystem in which the message itself is scrambled making use of a symmetric cryptosystem and El-Gamal is then used to encode simply the symmetric

key. This is due to the fact unbalanced cryptosystems like El-Gamal are usually slower than symmetric ones for a similar degree of protection, so it's far quicker to encode the message, which may be subjectively widespread, with a symmetric determine, and after that usage El-Gamal just to scramble the symmetric key, which more frequently than not could be very little contrasted with the dimensions of the message. The El-Gamal Algorithm offers an choice in comparison to the RSA for open key encryption.

- Security of the RSA is predicated upon the (assumed) trouble of figuring large entire numbers.
- Security of the El-Gamal calculation is predicated upon the (assumed) problem of registering discrete logs in an extensive prime modulus.
- El-Gamal has the detriment that the ciphertext is two times the period of the plaintext. It has the little bit of leeway the equivalent plaintext offers an alternate determine content material (with near sureness) every time its miles encoded.

El-Gamal encryption is one of numerous encryption plans which makes use of randomization within the encryption process. Others contain McEliece encryption (x8.Five), and Goldwasser-Micali (x8.7.1), and Blum-Goldwasser (x8.7.2) probabilistic encryption. Deterministic encryption plans, as an example, RSA may also likewise make use of randomization in order to pass around certain attacks and x8.2.2The key thought at the back of randomized encryption techniques is to make use of randomization to construct the cryptographic protection of an encryption process thru at the least one of the accompanying strategies – Increasing the compelling length of the plaintext message area; Precluding or diminishing the adequacy of picked plaintext assaults by means of goodness of a one-to-many mapping of plaintext to figure content; and Precluding or diminishing the viability of actual attacks via leveling the from the earlier likelihood conveyance of facts resources.

## IV. RESULTS AND DISCUSSION

The below results shows the outputs of project.

Users View page


**Figure 2**: Users view page.

Requested Files

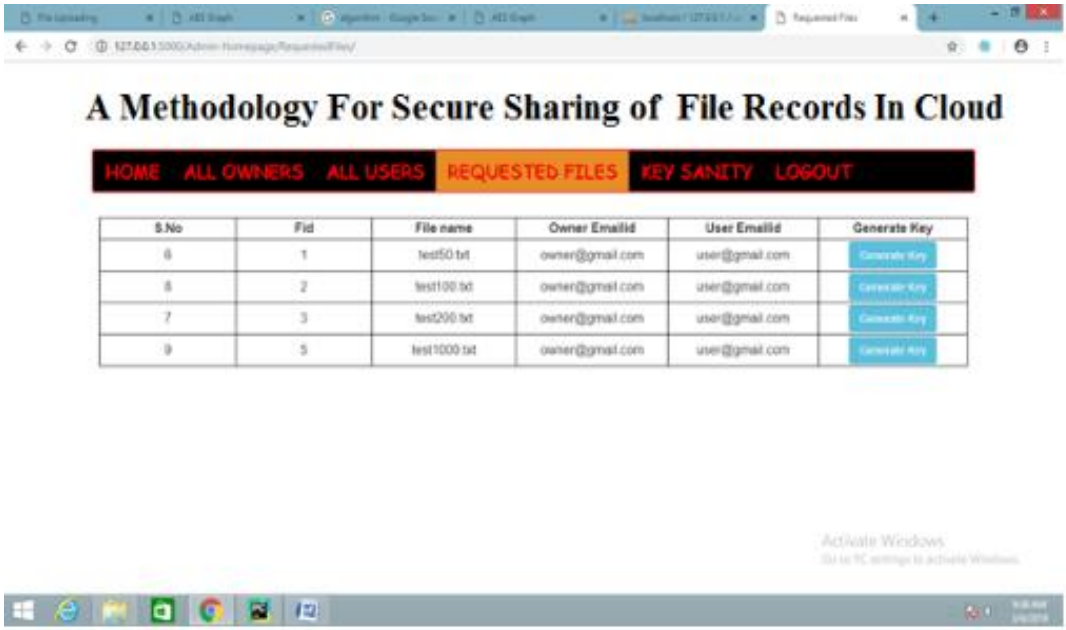


**Figure 3**: Requested Files page

File Upload and choosing an algorithm


**Figure 4**: File Upload and choosing an algorithm page

Time consumptions for Encryptions using AES Algorithm

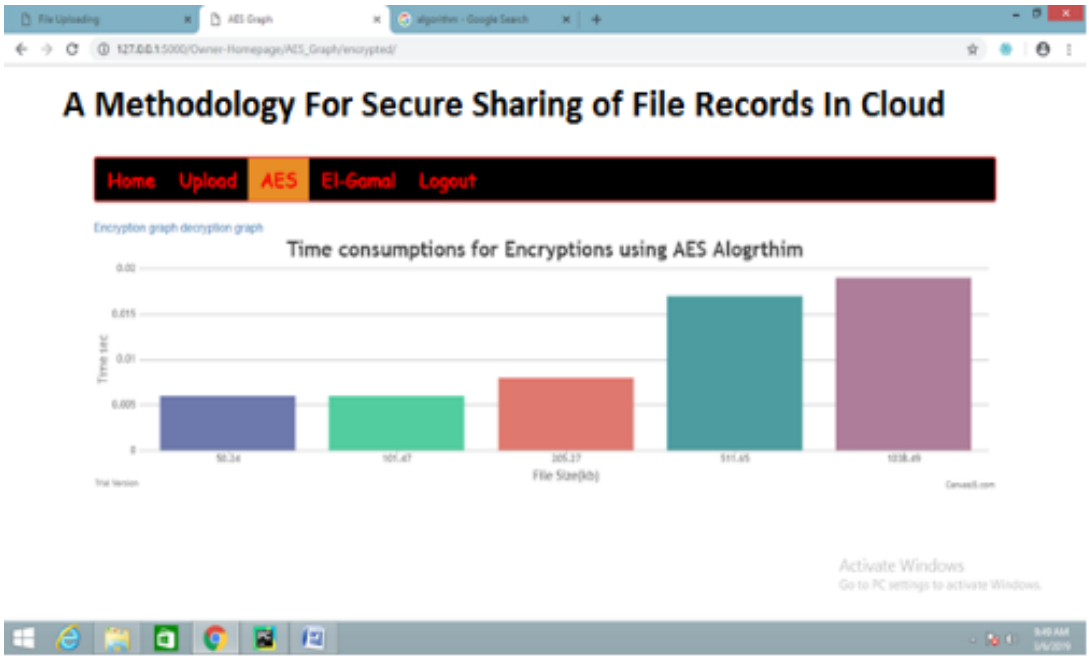


**Figure 5**: Time consumptions for Encryptions using AES Algorithm

Time consumptions for decryptions using AES Algorithm

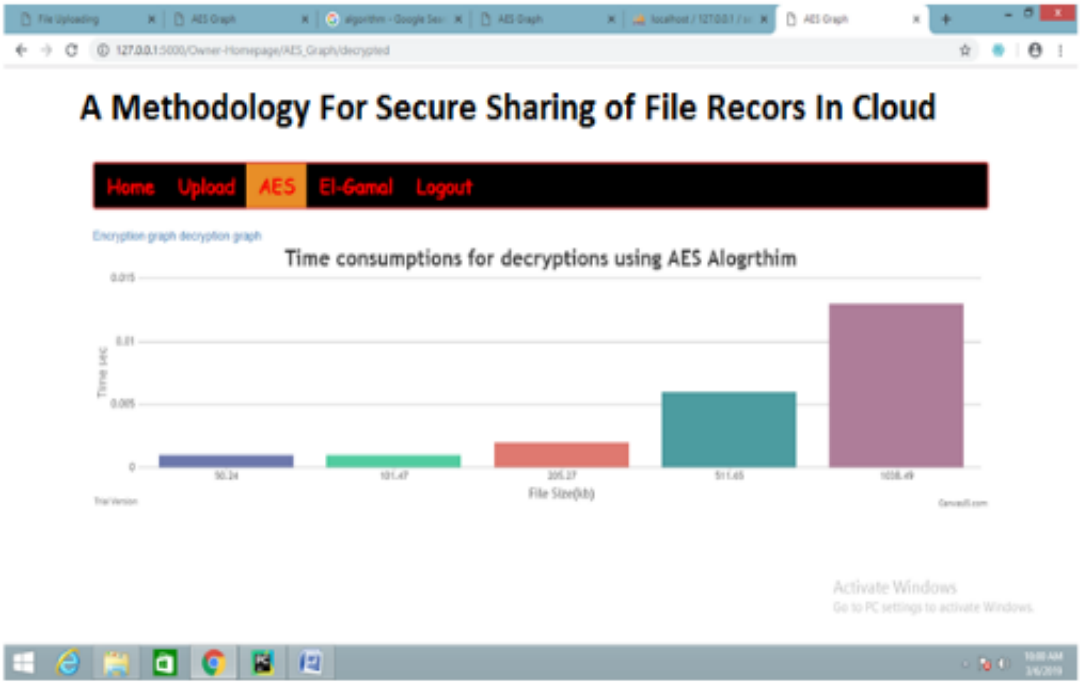


**Figure 6**: Time consumptions for decryptions using AES Algorithm

Time consumptions for Encryptions using El-Gamal Algorithm

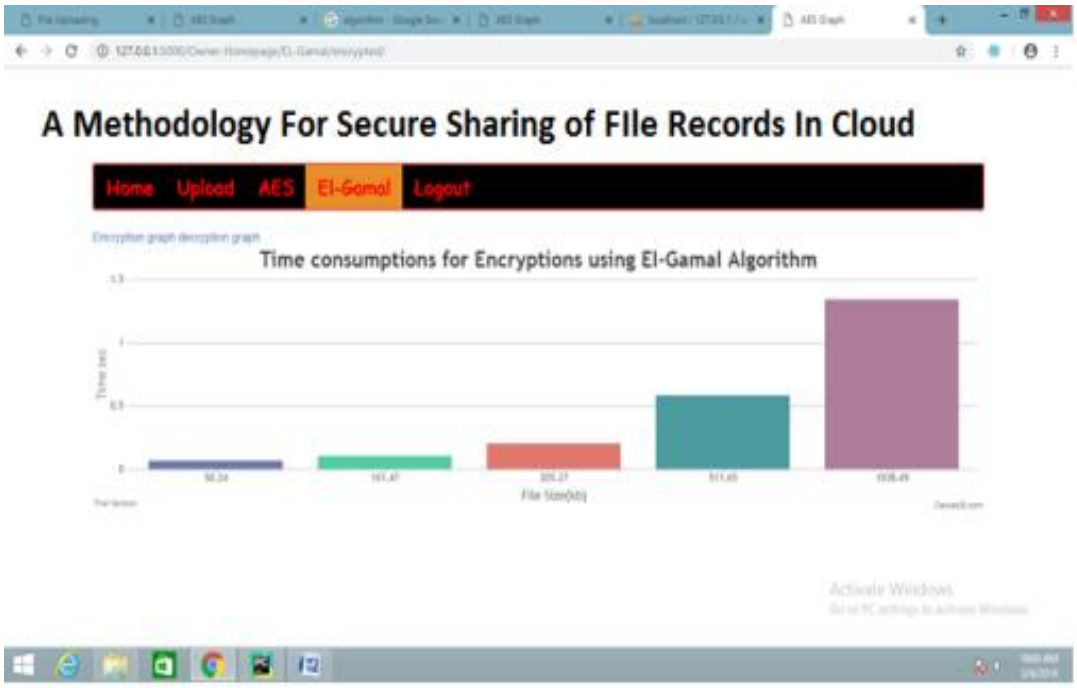


**Figure 7:** Time consumptions for Encryptions using El-Gamal Algorithm

Time consumptions for decryptions using El-Gamal Algorithm

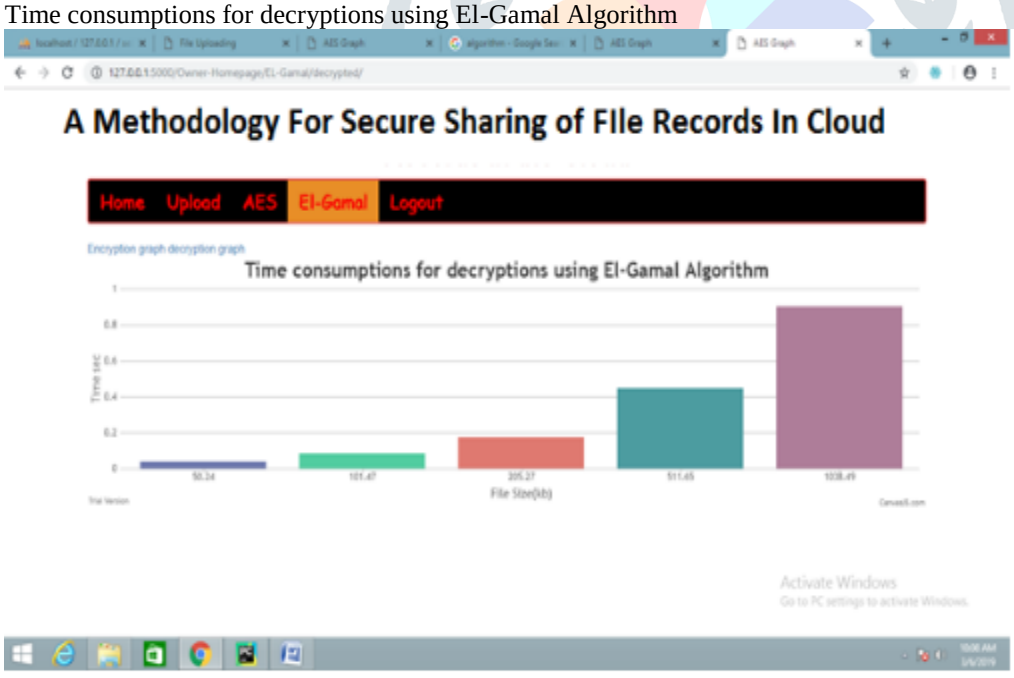


**Figure 8:** Time consumptions for Encryptions using El-Gamal Algorithm

Encryption Comparison of Time Consumption:

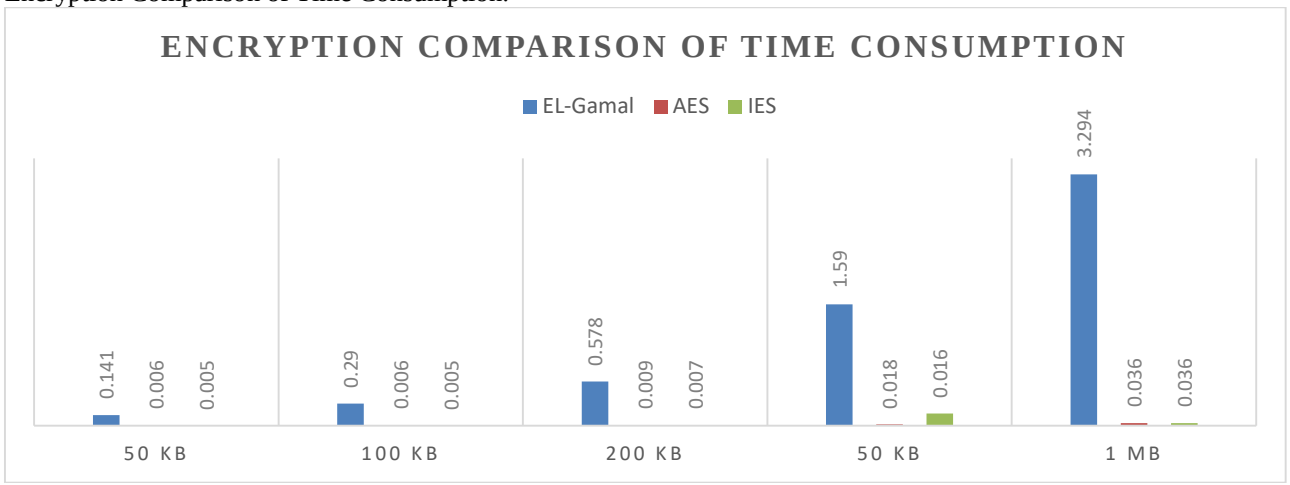


**Figure 9**: Encryption Comparison of Time Consumption

Encryption Comparison of Time Consumption:

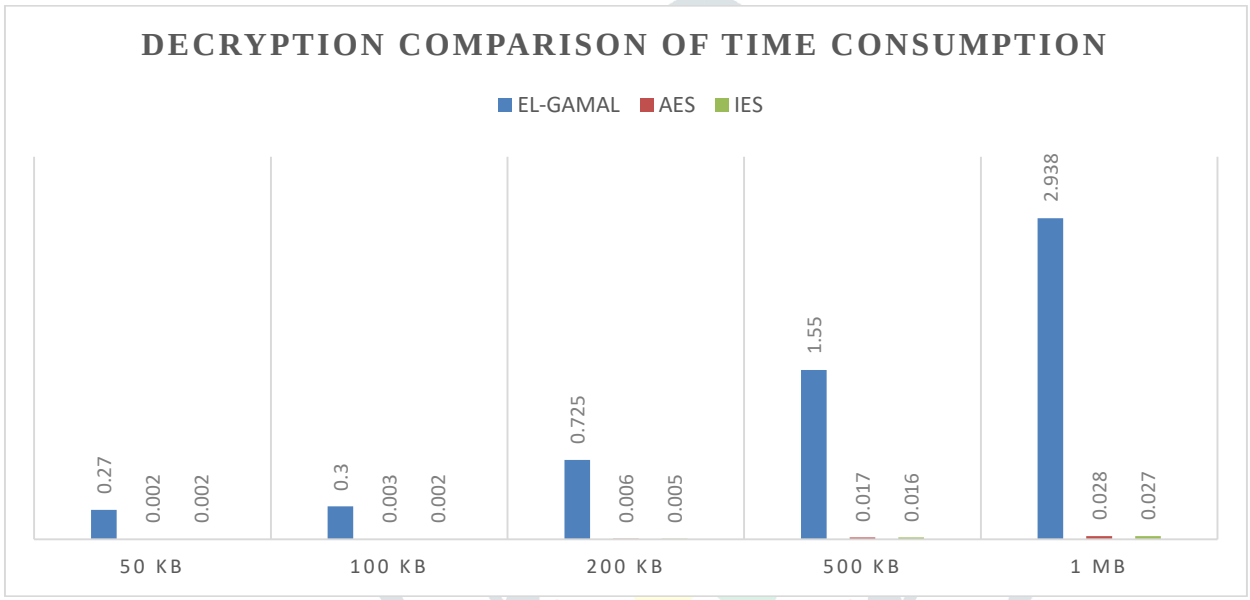


**Figure 10:** Decryption Comparison of Time Consumption

**Table 1** Time consumptions for Encryptions.

| Data Size | El-Gamal | AES | IES |
|---|---|---|---|
| 50 kb | 0.141 | 0.006 | 0.005 |
| 100 kb | 0.29 | 0.006 | 0.005 |
| 200 kb | 0.578 | 0.009 | 0.007 |
| 500 kb | 1.59 | 0.018 | 0.016 |
| 1000 kb | 3.294 | 0.037 | 0.036 |

**Table 2** Time consumptions for Decryptions

| Data Size | El-Gamal | AES | IES |
|---|---|---|---|
| 50 kb | 0.247 | 0.002 | 0.002 |
| 100 kb | 0.3 | 0.003 | 0.002 |
| 200 kb | 0.725 | 0.006 | 0.005 |
| 500 kb | 1.55 | 0.017 | 0.016 |
| 1000 kb | 2.938 | 0.028 | 0.027 |

## V. CONCLUSION

The passage manage and the assist of watchword search are large problems in calm dispensed capability gadget. The proprietors store the encoded realities on the cloud and essentially the allowed customers having genuine re-encryption keys issued with the aid of a semi commonplace mediator can unscramble The movement of the semi-familiar pass between is to deliver and maintain the general masses/non-open key units for the customers inside the device. Despite protecting the thriller and making sure statistics driven get right of passage to route over the way of wondering further controls the ahead and in inverse get right of section to supervise for pulling returned and the as of late becoming a member of customers, each one in turn. In this work, we described any other attitude of reachable encryption shape, and proposed a strong development.

## REFERENCES


**[1]** Ali, M., Abbas, A., Khan, U., & Khan, S. U. (2018).” *SeSPHR:* A Methodology for Secure Sharing of Personal Health Records in the Cloud”. IEEE Transactions on Cloud Computing

**[2]** Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Deen. “Privacy-preserving Double-Projection Deep Computation Model with Crowdsourcing on Cloud for Big Data Feature Learning,” IEEE Internet of Things Journal, 2017.

**[3]** R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, “Dual-Server PublicKey Encryption with Keyword Search for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 789-798.

**[4]** X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. ”An efficient privacypreserving outsourced calculation toolkit with multiple keys.” IEEE Transactions on Information Forensics and Security 11.11 (2016): 2401-2414.

**[5]** B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, 2004.

**[6]** Y. Yang, X. Liu, R.H. Deng, “Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language”. IEEE Transactions on Dependable and Secure Computing, 2018, publish online.

**[7]** W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, “Protecting Your Right: Verifiable Attribute-based Keyword Search with Finegrained Owner-enforced Search Authorization in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no. 4, pp. 1187-1198

**[8]** K. Liang, W. Susilo, “Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981- 1992.

**[9]** M. Green, S. Hohenberger, and B. Waters, “Outsourcing the decryption of ABE ciphertexts,” in USENIX Security Symposium, ACM, 2011, pp. 34-34.

**[10]** K. Gai, M. Qiu, Z. Xiong, and M. Liu, “Privacy-preserving multi-channel communication in Edge-of-Things,” Future Generation Computer Systems, 85, 2018, pp. 190-200.

**[11]** K. Gai, M. Qiu, and X. Sun, “A survey on FinTech,” Journal of Network and Computer Applications, 2017, pp. 1-12.

**[12]** A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, “A cloud based health insurance plan recommendation system: A user centered approach, “Future Generation Computer Systems, vols. 43- 44, pp. 99-109, 2015.

**[13]** A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, “Incremental proxy re-encryption scheme for mobile cloud computing environment,” The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

**[14]** R. Wu, G.-J. Ahn, and H. Hu, “Secure sharing of electronic health records in clouds,” In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-sharing (CollaborateCom), 2012, pp. 711-718.

**[15]** A. Abbas and S. U. Khan, “A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds,” IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.

**[16]** M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, “A general framework for secure sharing of personal health records in cloud system,” Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017.

**[17]** J. Li, “Electronic personal health records and the question of privacy,” Computers, 2013,

**[18]** D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, “A research agenda for personal health records (PHRs),” Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

**[19]** S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable and fine-grained data access control in cloud computing,” in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.

**[20]** S. Kamara and K. Lauter, “Cryptographic cloud storage,” Financial Cryptography and Data Security, vol. 6054, pp. 136–149, 2010.