A Novel Watermarking and Re-Encryption Approach to Avoid Illegal Content Sharing In Cloud

Pavithra G[a], Dhavasumani K[b], Keerthikumar R[c], Manoj S[d], Parthiban C[e]

[a]Department of Computer Science and Engineering ,M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India -639113
[b,c,d,e]Department of Computer Science and Engineering , M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India -639113
pavithrag.cse@mkce.ac.in ,
dhavasumanik2000@gmail.com,rkeerthikumar2000@gmail.com,manojsrinivasan3473@gmail.com,parthibanmuthu888@gmail.com

Article History: *Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021*

Abstract: Cloud computing is a set of information stored in a cloud, it can be accessed by the user whenever there is a need to access. Cloud computing is a combination of large interconnected computers. Importance of clod computing are storage and processing power to run application. Information can be access from anywhere .Data management is also one importance of the cloud computing. It improves performance. And also a lower infrastructure cost. Lower bandwidth does not support. Another important disadvantage is security thread. Cloud computing requires a constant internet connection. By using watermarking and re-encryption technique we can overcome the problem of security thread in the cloud. In this article we briefly discuss about the above mentioned technique for implementing to overcome the security thread in the cloud computing.

Keywords: Watermarking, Encryption, illegal, cloud, content sharing

1. Introduction

In today the users are access different system, services and application that are increasing the multimedia usage[1].The content provider normally have access to cloud computing for content sharing and hosting because of more media content is generated[2],[3]. In spite of having many benefits it have security issues [4], [5], [6]. Cloud storage data disclosure periodically happens [7].Sharing of media by cloud with embed security. Authorized persons only access the data others could not be access the data. There are two approaches are there for authorization. The starting method is depend on attribute-base encryption[8],[9],[10],[11].To access media send by the content provider the receiver should specify the pass key send by the content provider[12],[13].By using the PRE method illegal data sharing is avoided[14].The digital watermarking technique is used for tracing illegal content distribution[15],[16],[17].It works adding a distinct watermark of empty media description, Afterword's finding the previous watermark from an anonymous copy for informer detecting. This is the key method of watermarking. It has some restriction unkind content provider could structure uncomfortable from committing of leaking a media entity. For this trouble, we have a solution to overcome this trouble, client can able to ask against illegal actions. This reasonable specification help to the after progress of impartial watermarking methodology[18],[19],[20],[21],[22],[23].In later analysis n watermarked duplicate of every media article in the design was not possible, also tolerate from fault-finding extensibility problem due to demand of constant no of client. By combining proxy re-encryption and watermarking technique we are able reduce the watermark copies problem. We build monitoring that the cipher texts in proxy re-encryption keep up homomorphy operations [24], [25], [26].

2. Technical Backgrounds

2.1. WATER MARKING

The term digital watermarking was early stages mentioned in two term: "water mark". Alternatively highly secret or hide conveying or information protection, digital watermark is abstract explicit pattern insert in digital information using the embedded algorithm and an embedded key. Watermarking was the procedure of the beating digital data in a bearer signal. Watermark data could be retrieve by the detection key using the detection algorithm. It also used for detect the holding of the copyright of signal.

2.2. PROXY RE-ENCRYPTION

Which translates cipher texts from one encryption key to another encryption key is called as proxy re-encryption key and also it is known as cryptographic primitive. To share the encrypted message for the potential user without having the expose the clear text. To avoid compromising the private keys of the sender and the recipient, the re-encryption method should be a key independent. The unidirectional and do not require delegators to reveal their entire secret key to anyone is the primary advantage of this PRE scheme. By make use of re-encryption key RK proxy re-encryption algorithm convert a cipher text by using a public key PKA to cipher text PKB. The corresponding clear text did not know by server, because of decrypted by different key KA and KP in the PKA and PKB.

2.3. CRYPTOGRAPHY

Technique of protecting information and communication by use of codes is called cryptography. Cryptography is a process of transforming unintelligibletext from plain text and vice versa. Cryptography is one of the mechanism in watermarking method that is used to hide the digital information and also it provides high security. The prefix “crypt” means “hidden” or “vault” and the suffix “graph” stands for “writing”. In the cryptography method it have a two different methods that are Symmetric and Asymmetric methods. Asymmetric cryptography is a public-key cryptography. One public key, one private key-to encryption and decryption a message and protect it from access or use.

3. REVIEW

3.1. EXISTING SYSTEM ARCHITECTRE

In existing watermarking work by start undetectable adding a uncommon watermark in each duplicate of the ordinary media data.It helps to finding the existing of the uncommon watermark from a doubtful duplicate for informer detecting.

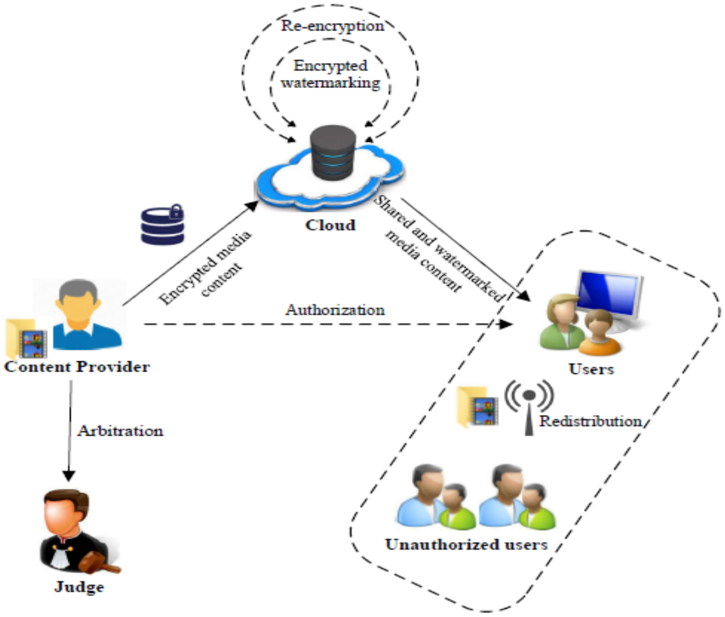

Figure 1:Architecture of Existing Systemmodel.

To keep up approach for secured media share in the encoded cloud data centre with help of attribute-based encryption (ABE) approach. Here content provider can describe an associated approach model over allocate, and this the cipher text store the cloud can only be decoded by client whose allocate convince that approach model.

Implement the first attempt towards privacy-preserving image noise reduction from outsourced cloud databases. In view of the image noise reduction demands top quality same as image stain, proposed design makes upon prior development on secured similar search, Yao’s garbled circuits, and image noise reduction operation, design for the best performance. To refine false-positive user at the cloud based side, we retreat to the appeal of Yao’s garbled circuits, which the execution has been regularly improve over the year. Particularly, the additional server we establish assemble garbled circuits for the cloud, who can acts as an export to securely correcting whether the interval between the reservation strain and user strain are within the starting point. With a secured garbled circuit based design that prevents against both cloud and the additional server, we can allow the cloud to discover the accurately and securely, without interactions with the user.

Proposed enables to the cloud providing encoded databases to provide secured query-based image noise reduction services. Leveraging the encoded equality search connecting SSE and LSH as our beginning point, we design and implement a secured estimating protocol depend on Yao’s garbled circuits to make sure that related stain are correctly acquire formal safety survey has been provided to valid security warranty of our model, and large observation over real-world database have illustrate that our model can accomplish the noise reduction aspect close to the minimum execution in plain text.

3.2. PROPOSE A NOVEL BIDIRECTIONAL PROXY RE-ENCRYPTION

The following properties are hold by the bidirectional proxy re-encryption scheme and it constant how many times the transformation is size no matter is performed. There are three properties usually required in cryptographic clod storage. That are master secret security and replayable chosen cipher text. The cloud server is assumed to be any user in the system in the application of cryptographic cloud storage. Based on pairings recently, proposed two BPRE schemes. Where the secret security Alice the proposed BPRE scheme. Where Alice colluding with the proxy cannot bob private key. Design a new grid to provide information in smart framework by providing current advantages in homomorphic encryption, proxy re-encryption. Design grid authorize energy supplies to control provider information while confirm the provider security. This work was proposed only on how the electric power consumption announce are secured sharing among the issued generation supplies. We grasp cons of the (DaaS) Data-as-a-Service method in cloud computing the Trusted Authority (TA), more Electricity Consumers (ECs), more Energy Resources (ERs), cloud servers. For creating the system specification and the certificates for the public key of every Energy Resources. The electric power utilization announce that are redistribute to the cloud servers. To fulfill the enhanced security, the electric utilization announce could be encoded by applying the public key of the related ER where the utilized electric power came from. Beneficial to design a clever determination on the electric power creation, cost and others, every ER should like to do survey on the electric power utilization announce particularly to oneself or another ERs. Prior to performing the evaluation, the ER would acquire the evaluation license from another ERs.

Specific the cloud server was absorbed to gathering the information of electric power utilization announce or survey report, but they will not change the conveying information with another establishment or scheme with other establishment. The ERs desire to obtain the evaluation report from the cloud servers so that they can proposal many excellently and accurately to make a sufficient supply of electric power to provide their local demand. It takes a major role in create our power framework more dependable and adaptable since we should maintain the framework by matching electric power provide with a demand absolutely to avoiding the electric power framework collapse. Malicious ERs may approach electric power utilization result or get the evaluation report far away their evaluation license.

3.3. HOMOMORPHIC PROXY RE-AUTHENTICATORS

To adding privacy guarantee and sustainable warranty too many-client information gathering scenarios by using tool of homomorphic proxy re-authenticators. To validate their information undergoing their admit key. It allows from distinct sources, a proxy can transform the message authentication or single signatures codes to a MAC undergoing a beneficiary’s key doesn't have entrance to it.MAC corresponds to evaluation of the respective function, because of proxy could estimate arithmetic loop(functions) on the inputs. Hiding sensitive information that are authenticated by source belongs to the proxy and another groups in the system, omitting from beneficiary. Modify an information m encoded undergoing universal key rpkA of party A into cipher text to m undergoing rpkB for other group B from a proxy is called proxy re-encryption (PRE) scheme.

locally approach to individual key and only B’s universal key when there is group A can make a re-encoded key for B, from A, when PRE scheme is called non-interaction, the proxy collaborate with any one of the groups cannot retrieve the another group individual key is called collusion-safe unidirectional if a re-encoded key only allows modification in one way of direction (e.g., from A to B), and single-use if one cipher text could be modified only once. To fetch the encoded files of scrutiny, more searchable symmetric encryption (SSE) strategy have been suggested. The popular methodology for SSE solutions construct indexes depend on keyword-file pairs and concentrate on Boolean expressions of specific keyword matches. Furthermore most dynamic SSE solutions unable to accomplish forward privacy and leak unwanted data when refurbish the encoded databases. Suggest infusion are construct on warily waggish Bloom riddle which use locality sensitive hashing (LSH) to encrypt an index connecting the file identifiers and aspect vectors. These strategies are proven to be stable against flexible chosen query strike and forward individual in the quality prototype

The key concept is to remold the information into a set of component vectors, which are further merged by LSHs to an array location. We call the starting point there a bucket, which will be referring to the feasible equal files. Since the LSH transfers all related files to the same output, together with our unique treatment of generation it hence produce a bunch of buckets which carry files roughly close to the query object with a maximum possibility. To illustrate the pointers to the file, we store the upend file identifier vectors (IFVs) in each of this bucket. An Identifier vector is a vector which indicates the set of data that drop in a given bucket for one hash function. For exchange of estimating capability and bandwidth, we have two ways in encoding the emerging IFVs, which are addition homomorphic encoding (for saving bandwidth) or pseudo-random functions/permutations (for more structured computation). The emerging strategies enable the user to perform security-conserving equivalent search by inspecting only a few number of hash tables (or buckets). The reaction set consists of exact files which can be instantly used for security conserving KNN or approximate nearest neighbors (ANN) search. Other systematic and bewitching property of our index establishing is that they are highly compact, neat and efficient, and they can also skillfully keep up secure dynamic renovate of set of data and index with minimum functioning

4. PROPORSE SYSTEM ARCHITECTURE

To suggest a new system model authoring encryption pointing in mobile mass sense security model is assemble the confidence-aware truth discovery (CATD) model for its state-of-the-art correct in such conditions System architecture, Client send encoding sensitive information to the cloud, where CATD is then organized in the encoded domain. The sensitive information and accuracy degrees of client, as well as the key requester, are kept safe .Suggest the security system grid for encoded trust -aware truth finding in mobile mass sensing. It can disturb highly exact realistic data, while giving client privacy and requester preservation. Then present a basic establishment for encoding trust aware truth finding as beginning point, and further give our improved establishment with minimized communication difficult between the two cloud servers.

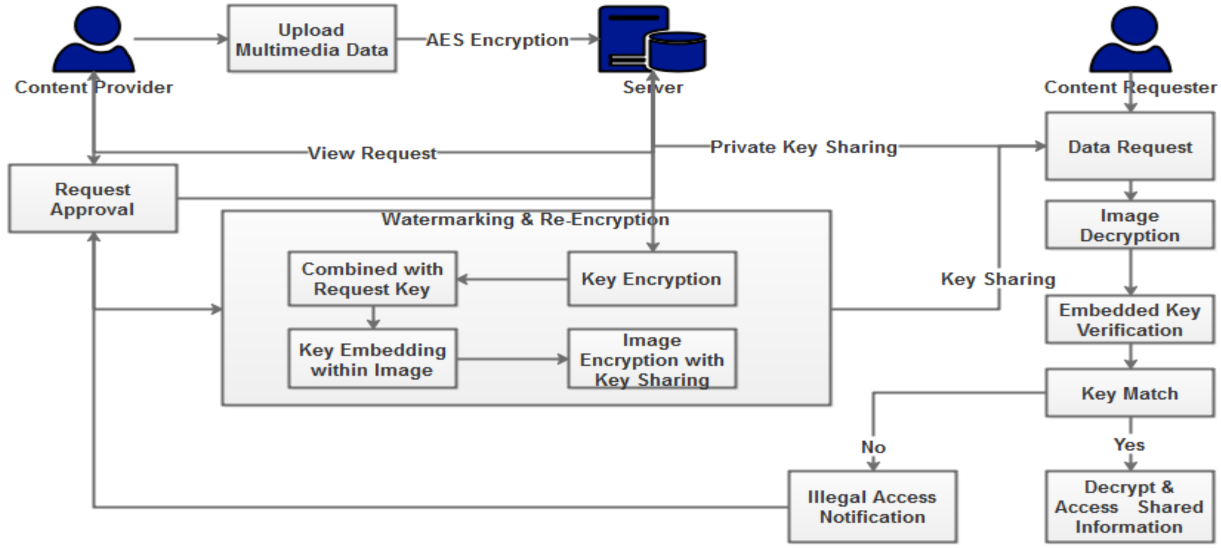
Content Provider
Upload Multimedia Data
AES Encryption
Server
Content Requester
View Request
Private Key Sharing
Data Request
Request Approval
Watermarking & Re-Encryption
Image Decryption
Combined with Request Key
Key Encryption
Key Sharing
Embedded Key Verification
Key Embedding within Image
Image Encryption with Key Sharing
Key Match
No
Yes
Illegal Access Notification
Decrypt & Access Shared Information

Figure 2: Flow diagram for proposed system model.

In this system, we review that the cloud establishment consists of both cloud servers S0, S1, which are organized by unconventional cloud service vendors. Both-server replica has been widely acquire in the literature to promote secured technology and we regard our acquire of this replica to be in this current. In suggested model, S0 serve mass sensing domain that discharges the objects from the applicant, and gather encoded sensing utility from clients, while S1 apparently deliver estimation assist to S0 to keep up encoded CATD. When encoded CATD is completed, S0 send the encoded reason to the applicant for decoded. It is virtue nothing that in our model the applicant and client are not needed to remain online to interactively present in the encoded CATD method. To implement a new query processing protocols and privacy-preserving indexing which reach a many possessions, together with the disjunction logic queries and many-keyword query preparing with concurrence, practically high privacy guarantees of the dynamic data operations and security are adaptive chosen keyword. Based on of information identifier vectors, we approach an encoded approach which permit discovery of data to equal the public many-keywords query. Our key proposal is as come after. Subsequently, both conjunctive and disjunctive relationship queries can be executed by doing arithmetic functions on the DIVs strike by the supply analyze representation, which is similar to post-preparing an arrangement of unique-keyword queries. Particularly, for the united logic queries, data's are come back if the meeting of all hit chunk in a row same as to 1. Based on above ideas, the plan BEIS-I and BEIS-II security protection for further process. The earlier masking with outputs of a Permit-vectors paillier homomorphic cryptosystem. Intuitively, BEIS-I is estimatly more efficient because to the usage of symmetric encryption, while BEIS-II has underneath conveying value since the cipher text packing technique is adopted. Suggest a compressive sensing (CS)-based grid utilize secured multiparty computation (MPC) protocols to pointing such a needs. Our structure, interactive media information and mystery watermark design are introduced to cloud for secured watermark disclosure in a compressive sensing space to guarantee insurance. Applying CS modification, the security of the CS matrices and the watermarked method is secured by the MPC method under the semi-honest security protocol. We infer the normal watermark discovery execution in the compressive sensing space, given the objective picture, watermark design, and the magnitude of the CS grid (however except the CS network themselves).In the grid, the desired result image information is owned by the image owner only. A compressive sensing matrices is provided by a certificate authority (CA) server to the image owner. The picture owner changes the DCT factor of the picture information to a constrictive detecting area in front of re-appropriates it to cloud. For secured watermark perception, the watermark is modified to the selfsame compressive sensing area used a secured multiparty computation (MPC) model and then transferred to cloud. Cloud just has the information in constrictive finding space. Except the constrictive sensing matrices, the cloud could not disclose the initial multimedia information and watermark model. Cloud would execute watermark identification in the constructive detecting area. The image information in the constructive observing field can be saved in the cloud, reutilize for finding of watermark from more another watermark holders. Proposed framework is protect under the partially-fair presumption that's all gatherings follow the convention's system carefully, and nothing will effectively pull out halfway or fuse bogus or noxious information. Not two gatherings will plot to assault a third one. In any case, during the figuring interaction, they may attempt to keep all the moderate data, so we can surmise another's' contribution later cycle. Partially-legitimate method is a sensible presumption for foes, for example, outsider specialist co-ops .suggest a plan that keep up CBIR over encoded images except distribute the secure data to cloud servers. Initially, properties vectors are obtained to point out the similar images. Consequently, the before-filter buckets is built by locality-sensitive hashing to improve detect effectiveness. In addition, the property vectors is secured by safe knn Algorithm, and image component are encoded by a fixed Stream Cipher. Moreover, in view of the expression that the approved content providers may criminally duplicate and deliver the received images to anyone unapproved, so we suggest a watermark-based model to deter such actionable delivery. In watermark-based model, an individual watermark is straightly embed into encoded images for the cloud servers in front of images are transmit to receiver side. When a no legal duplicate image is detected, the third-party client who delivered the image can be tracked by the watermark removal method.

For the duplicate-discourage reason, we required to add a watermark towards all the received images for every query demand. It needs a more estimation effort and thus is awaited to be finished by the cloud server. Consequently, we required to enhance a watermarking approach that is well organized and add the watermark straightly in the encoded image by cloud servers. Behind collecting the encoded and watermark images, the inquiry client should be access to straightly decode the watermark images with the predetermined confidential keys. After the decoded, the watermark will be in images. In a watermark-based duplicate prevention model, the content provider may asperse a inquiry client by embedded the watermark relevant to the client in initial images. The suggested models requires to protect the model of nonleague manners.

Which connecting both the elevation of video coding method and secured copy are current secured system architecture model as our beginning involvement with regard to this phase. This proposed model allows the cloud with critical duplication usability to entirely terminate the unwanted memory and transmission capacity value, which would have been sustain by organizing encoded video from dissimilar operation**.** Replication is critical for the encoded cloud media center to terminate the inconvenient memory and transmission capacity overhead when keeping encoded videos from multiple clients. Proposed model point secured origin-based replication, where the unwanted video is terminate at the origin base. Many valuable, the transformation of replica videos would be saved before replica evaluate is achieved clients update their encoded videos. Towards supply powerful video conservation in the encoded cloud media center, we utilize to a firm server for assistance in our model, carry on the dependability power of the over procedure while ignoring its undefended. An OPRF model is begin linking the client and the firm server, manufacturing a set of information-obtain label α and badge. The badge α, rather of the plaintext hash, is worn for replication evaluate in cloud. And the tag β is added in the one-time information-obtained assists recovery of spontaneous key τ through the succeeding update of a replicate video and hide through the beginning the update of a new video.

5. Future Work and Conclusion

As a promising primitive to secure the data sharing in th cloud computing, PRE has captured a lot of concern due to the delegation function of decryption. In this paper, we checked on the best in class of the PRE by examining the plan reasoning, inspecting the security models, and contrasting the efficiency of existing plans. Furthermore, the potential applications and extensions of PRE have also been discussed.There are some conceivable fascinating issues with regards to this exploration field that need further investigation, One direct open issue of PRC is the way to plan a nonexclusive structure which can change the customary encryption/mark to intermediary re-encryption/re-signature Finding the efficient PRE plans with full security is additionally an open issue since the vast majority of the current PRE plans can just accomplish particular security. Identifying new scenarios where the decryption/signing rights of the resource-limited users can be delegated to the resource-abundant proxy by adapting the existing PRC schemes to feature with special properties can be regarded as another open problem.

References

C. P. Chen and C.-Y. Zhang, "Data-intensive applications, chal- lenges, techniques and technologies: A survey on big data," Infor- mation Sciences, vol. 275, pp. 314–347, 2014.

W. Zhu, C. Luo, J. Wang, and S. Li, "Multimedia cloud computing," IEEE Signal Processing Magazine, vol. 28, no. 3, pp. 59–69, 2011.

H.Xiong, X. Zhang, D. Yao, X. Wu, and Y. Wen, "Towards end- to-end secure content storage and delivery with public cloud," in Proc. of ACM CODASPY, 2012, pp. 257–266.

Murugesan, M., Thilagamani, S. ," Efficient anomaly detection in surveillance videos based on multi layer perception recurrent neural network", Journal of Microprocessors and Microsystems, Volume 79, Issue November 2020, https://doi.org/10.1016/j.micpro.2020.103303

Y. Zheng, H. Cui, C. Wang, and J. Zhou, "Privacy-preserving image denoising from external cloud databases," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1285–1298, 2017.

Z. Shan, K. Ren, M. Blanton, and C. Wang, "Practical secure computation outsourcing: A survey," ACM Computing Surveys, vol. 51, no. 2, pp. 31:1–31:40, 2018.

Thilagamani, S., Nandhakumar, C. ." Implementing green revolution for organic plant forming using KNN-classification technique", International Journal of Advanced Science and Technology, Volume 29 , Isuue 7S, pp. 1707–1712

J.Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. of IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

Thilagamani, S., Shanti, N.," Gaussian and gabor filter approach for object segmentation", Journal of Computing and Information Science in Engineering, 2014, 14(2), 021006, https://doi.org/10.1115/1.4026458

F.Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption," Multimedia Tools and Applications, vol. 74, no. 10, pp. 3441–3458, 2015.

Rhagini, A., Thilagamani, S. ,"Women defence system for detecting interpersonal crimes",International Journal of Advanced Science and Technology, 2020, Volume 29,Issue7S, pp. 1669–1675

1. *K. Liang, W. Susilo, and J. K. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1578–1589, 2015.*
2. *K.Deepa, S.Thilagamani, "Segmentation Techniques for Overlapped Latent Fingerprint Matching", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-12, October 2019. DOI: 10.35940/ijitee.L2863.1081219.*
3. *Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," IEEE Transactions on Services Computing, in press, 2016.*
4. *J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673–1687, 1997.*
5. *Deepa, K., Kokila, M., Nandhini, A., Pavethra, A., Umadevi, M. "Rainfall prediction using CNN", International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1623–1627. http://sersc.org/journals/index.php/IJAST/article/view/10849.*
6. *Santhi, P., Mahalakshmi, G., Classification of magnetic resonance images using eight directions gray level co-occurrence matrix (8dglcm) based feature extraction, International Journal of Engineering and Advanced Technology, 2019, 8(4), pp. 839–846*
7. *Vijayakumar, P, Pandiaraja, P, Balamurugan, B & Karuppiah, M 2019, 'A Novel Performance enhancing Task Scheduling Algorithm for Cloud based E-Health Environment', International Journal of E-Health and Medical Communications , Vol 10,Issue 2,pp 102-117*
8. *N.Memon and P. W. Wong, "A buyer-seller watermarking pro- tocol," IEEE Transactions on Image Processing, vol. 10, no. 4, pp. 643–649, 2001.*
9. *Santhi, P., Lavanya, S., Prediction of diabetes using neural networks, International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1160–1168.*
10. *M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for im- ages based on additive homomorphic property," IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2129–2139, 2005.*
11. *Rial, M. Deng, T. Bianchi, A. Piva, and B. Preneel, "A provably secure anonymous buyer–seller watermarking protocol," IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 920–931, 2010.*
12. *Santhi, P., Priyanka, T.,Smart India agricultural information reterival system, International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1169–1175.*
13. *G.Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure dis- tributed storage," ACM Transactions on Information and System Security, vol. 9, no. 1, pp. 1–30, 2006.*
14. *P. Pandiaraja, N Deepa 2019 ," A Novel Data Privacy-Preserving Protocol for Multi-data Users by using genetic algorithm" , Journal of Soft Computing , Springer , Volume 23 ,Issue 18, Pages 8539-8553.*
15. *D.Derler, S. Ramacher, and D. Slamanig, "Homomorphic proxy re-authenticators and applications to verifiable multi-user data aggregation," in Proc. of International Conference on Financial Cryp- tography and Data Security, 2017, pp. 1–24.*
16. *N Deepa , P. Pandiaraja, 2020 ," Hybrid Context Aware Recommendation System for E-Health Care by merkle hash tree from cloud using evolutionary algorithm" , Journal of Soft Computing , Springer , Volume 24 ,Issue 10, Pages 7149–7161.*
17. *Peter, E. Tews, and S. Katzenbeisser, "Efficiently outsourcing multiparty computation under multiple keys," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2046–2058, 2013.*
18. *N Deepa , P. Pandiaraja, 2020 , " E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption ", Journal of Ambient Intelligence and Humanized Computing , Springer , https://doi.org/10.1007/s12652-020-01911-5.*
19. *Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, "Searchable encryption over feature-rich data," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 496–510, 2018.*
20. *K Sumathi, P Pandiaraja 2019," Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks" , Journal of Peer-to-Peer Networking and Applications , Springer , Volume 13,Issue 6,Pages 2001-2010.*
21. *Shao, Jun, Rongxing Lu, Xiaodong Lin, and Kaitai Liang. "Secure bidirectional proxy re-encryption for cryptographic cloud storage." Pervasive and Mobile Computing 28 (2016): 113-121.*
22. *Alharbi, Khalid Nawaf, Xiaodong Lin, and Jun Shao. "A privacy-preserving data-sharing framework for smart grid." IEEE Internet of Things Journal 4, no. 2 (2016): 555-562.*
23. *Derler, David, Sebastian Ramacher, and Daniel Slamanig. "Homomorphic proxy re-authenticators and applications to verifiable multi-user data aggregation." In International Conference on Financial Cryptography and Data Security, pp. 124-142. Springer, Cham, 2017.*
24. *Wang, Qian, Meiqi He, Minxin Du, Sherman SM Chow, Russell WF Lai, and Qin Zou. "Searchable encryption over feature-rich data." IEEE Transactions on Dependable and Secure Computing 15, no. 3 (2016): 496-510.*

25. Zheng, Yifeng, Huayi Duan, and Cong Wang. "Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing." IEEE Transactions on Information Forensics and Security 13, no. 10 (2018): 2475-2489.

26. Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., Sharma, P. ,” Privacy preserving E-voting cloud system based on ID based encryption ” Journal of Peer-to-Peer Networking and Applications , Springer , https://doi.org/10.1007/s12083-020-00977-4.

27. Wang, Qia, Wenjun Zeng, and Jun Tian. "A compressive sensing based secure watermark detection and privacy preserving storage framework." IEEE transactions on image processing 23, no. 3 (2014): 1317-1328.

28. Xia, Zhihua, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing." IEEE transactions on information forensics and security 11, no. 11 (2016): 2594-2608.

29. Zheng, Yifeng, Xingliang Yuan, Xinyu Wang, Jinghua Jiang, Cong Wang, and XiaolinGui. "Toward encrypted cloud media center with secure deduplication." IEEE Transactions on Multimedia 19, no. 2 (2016): 251-265.