IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-15, May 2019 E-ISSN: 2347-2693

Deduplication of Image at Client Side Using DICE Protocol

[1]Akshay R, [2]Ankith A K, [3]Amith B, [4]Jayanth R, [5]Kiran Mensinkai

Department of Computer Science ,East West Institute of technology, Vishveswaraya Technological University, Bangalore, India

DOI: https://doi.org/10.26438/ijcse/v7si15.3642 | Available online at: www.ijcseonline.org

***Abstract*—**With the approach of distributed computing, verified information de-duplication has picked up a ton of fame. Numerous methods have been proposed in the writing of this continuous research territory. Among these procedures, theMessage Locked Encryption (MLE) conspire is regularly referenced. Analysts have presented MLE based conventions which give verified de-duplication of information, where the information is by and large in content structure. Thus, sight and sound information, for example, pictures and video, which are bigger in size contrasted with content documents, have not been given much consideration. Applying tied down information de-duplication to such information documents could essentially decrease the expense and space required for their capacity. In this paper we present a safe de-duplication conspire for close indistinguishable (CI) pictures utilizing the Dual Integrity Convergent Encryption (DICE) convention, which is a variation of the MLE based plan. In the proposed plan, a picture is disintegrated into squares and the DICE convention is connected on each square independently as opposed to on the whole picture. As a result, the hinders that are normal between at least two CI pictures are put away just once at the cloud.

***Keywords*—**De-duplication, Storage system, DICE protocol, Cloud storage

I. INTRODUCTION

Distributed computing gives clients the stage to profitcloud benefits on interest which incorporate fundamentally capacity, database, systems administration, and programming administrations over the Internet.Regardless of whether a client is watching films, tuning in to sound, taking pictures, facilitating sites or making new applications, cloud registering is a necessary piece of every one of these administrations. Cloud specialist co-ops (CSPs) charge their clients an ostensible expense for the utilization of these administrations. Thusly, it is vital for the CSPs to keep up a tradeoff between the expense of the administrations they give and the expenses that they charge to their clients, as keeping up and putting away the tremendous volume of clients' information, alongside the transmission capacity utilization bring about expenses for the CSPs. CSPs depend on de-duplication procedures to evacuate copy information and along these lines lessen transmission capacity and capacity necessities. In any case, it is similarly vital for CSPs to guarantee the protection and security of clients' information. To address both these issues, verified information de-duplication was presented, in which copy information is evacuated while keeping up the privacy of the clients' information. A lot of research is being done in the field of secure information de-duplication [1], [2] The greater part of the protected information de-duplication methodologies found in the writing treat information in a conventional sense. In all actuality, information can be one of a few distinct sorts, for example, content, pictures and video information. Actually, sight and sound substance, for example, pictures and recordings include a noteworthy segment of any information storehouse, as the rate of sharing has expanded with simple availability of the Internet and the engendering of shrewd gadgets. Henceforth, deciding copy duplicates in the encoded picture and video information is a generous test.

The current strategies intended for nonexclusive information may not be legitimately reasonable for media information, due to not just its volume, assortment, speed and veracity, yet in addition how do we characterize deception in interactive media information. For instance, two pictures with little contrasts in certain squares (as appeared in Figure 1(a)) or with contrasting goals (as appeared Figure 1(b)) could be considered as close indistinguishable and would along these lines be a contender to be considered for de-duplication.

In this paper, we present a protected square dimension picture de-duplication strategy that kills the close indistinguishable pictures (formally characterized in Section 3) in scrambled structure, in this way securing the secrecy of the pictures. The proposed strategy embraces the Dual Integrity Convergent Encryption convention that the creators proposed in their ongoing work [3]. Our center thought is to separate the picture into squares and utilize the DICE convention on each square independently. Each square is encoded utilizing AES with a key that is acquired by hashing the picture squares.

This implies indistinguishable squares in any two pictures will produce the equivalent cipher-text, which enables the CSPs to perform de-duplication on the cipher-text squares. The correspondence what's more, transmission capacity necessities are additionally limited since just a single tag is produced from the cipher-text. The security of the plan has been dissected tentatively as well as hypothetically.

The rest of the paper is prepared as follows: section II says the related work in detail. In section III, we discuss the proposed method. Then we describe the security in section IV andperformance analyses in section V respectively. Finally, section VI concludes the paper witha discussion on the future work.

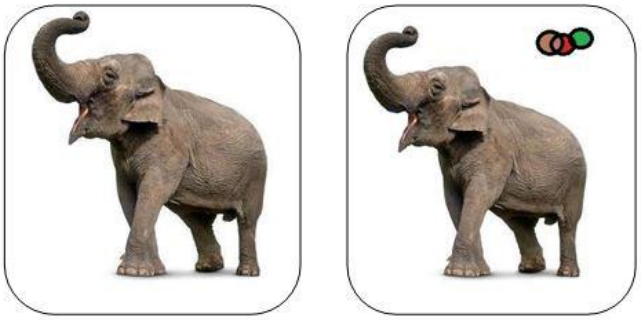

Figure 1: Two Closely indistinguishable images differing in some blocks

II. RELATED WORK

In this area, we talk about related work from two viewpoints: 1) cryptographic conventions that are proposed for secure information de-duplication, expecting that the information is nonexclusive, and 2) adaptions of these conventions for secure picture information de-duplication. From the cryptographic conventions perspective, Bellare et al. have proposed the Message Bolted Encryption (MLE) conspire [4], which characterizes the best in class convention principles. There are a few other MLE-based methodologies in the writing, for example, Joined Encryption (CE), HCE1, HCE2 furthermore, Randomized Joined Encryption (RCE) [5]. All of these methodologies give de-duplication along the fundamental cryptographic security viewpoints [6], [7]. Be that as it may, these systems are helpless against security assaults; among them explicitly referenced is the toxic substance assault which incorporates the copy faking assault and the eradication assault, where the vindictive enemy replaces the first record with the ruined one. Therefore, legit clients lose their documents and are lead to download the faked ones. A de-duplication system could be on the server side or on the customer side. In server-side de-duplication, the customer transfers the records (counting copies) to the server and at that point the server evacuates the copies and stores the one of a kind records likewise. In the meantime, the server approves the customer to get to the records and update the metadata. As an outcome, the overhead is higher on the server side and this prompts more data transmission utilization and calculation cost. On the other hand, in the customer side de-duplication system, the calculations are first done on the customer side by producing labels. The server is then sent just the labels rather than the whole document and further correspondence proceeds through tag checking. In the customer side de-duplication technique, the goal is to make less overhead at the server. Consequently, the customer side De-duplication procedure is progressively proficient, especially as the number of customers continues developing [8]. The two systems, customer side and server side, have their own advantages and disadvantages [9].

Agarwala et al. [3] as of late proposed the Bones convention which lessens the calculations, correspondence and transmission capacity necessities by consolidating only one tag. In this convention, the vast majority of the calculations were performed on the customer side. The de-duplication is performed at the record level, where the copy records are distinguished by applying hash works on the whole record and afterward checked if the hash values are the equivalent.On account of picture information, applying hash on the whole picture information may not be suitable, as the hash esteem may contrast regardless of whether two pictures are distinctive as it were by a pixel esteem, which crushes the objective of de-duplication. Or maybe, the picture documents could be disintegrated into squares and de-duplication can be performed by first applying hash on the squares, and afterward by checking the similitude between the hash benefits of comparing squares, which is the technique we actualize in this paper.

Secure de-duplication of pictures has been tended to by various scientists. For example, Posse et al. [10] thought about the de-duplication of the whole picture and connected the CE plot combined with Trait Based Encryption to perform picture de-duplication. In another work, Fatema et al. [11] utilized SPIHT pressure qualities and incomplete encryption alongside picture hashing to perform de-duplication.The fractional encryption plot gives security against the CSP and the picture hashing system recognizes the indistinguishable packed and scrambled pictures for de-duplication. In their work, the client originally connected the picture pressure calculation, at that point utilized the halfway encryption plot lastly figured the picture hash signature.The mark is then sent to the CSP to check for de-duplication. Another work by Li et al. [12], proposed a plot called Customer based Security Provable De-duplication of Interactive media Information (CSPD), which checked the duplicationof pictures utilizing fluffy techniques. Dissimilar to different methodologies thatcheck duplication on the picture hashes, in their technique,after the client transfers certain number of parameters of the picture to the CSP, the

CSP applies Hamming separation based on the parameters of the put away pictures and looks for comparable pictures in the database.In their work, Xuan Li et al. [13] propose a protected perceptual comparability de-duplication plot where they utilize the pHash calculation to decide the comparability of the picture hashes put away at the cloud by figuring the hamming separations between the put away picture hashes. They additionally utilize a gathering key, where all the individuals in a specific gathering can transfer and download the pictures utilizing the gathering key. The gathering keys are altogether kept what's more, utilized by the clients as indicated by the gathering of clients sharing information. Their plan is likewise powerful to basic picture preparing activities, for example, resizing and pressure. The vast majority of the work that we found in the writing is based on processing the hash of the whole picture without a moment's delay, rather thanchanging over the pictures into squares.

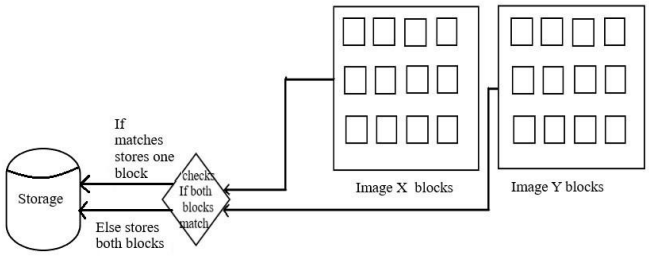

Figure 2: Block level deduplication of two images

Such plans are for the most part valuable for indistinguishable pictures, anyway they are not reasonable foralmost indistinguishable pictures. We trust that separating thepictures into littler structures like squares, considering the highlights of the squares and after that performingde-duplicationat the square dimension will altogether accomplish a more exact strategy for de-duplication. A secure de-duplicationscheme for Closely Indistinguishable (CI) images using the Dual IntegrityConvergent Encryption (DICE) protocol, which is a variant ofthe MLE based scheme. In the proposed scheme, an image isdecomposed into blocks and the DICE protocol is applied oneach block separately rather than on the entire image. As aresult, the blocks that are common between two or more NIimages are stored only once at the cloud[14].

III. METHODOLOGY

A. Closely Indistinguishable

In this work, we characterize the close indistinguishable picture situation as at least two pictures which have a similar foundation, however, there is either an adjustment in a specific square, or a few of the pixels are extraordinary. These contrasting pixels might be amassed in a particular district or might be dispersed all around the picture (two instances of close indistinguishable pictures are appeared in Figure 1). Beneath, we give a formal definition of close indistinguishable pictures. Definition 1: δ-CI Images: A picture pair (I, I) is called δ-CI (or δ-close indistinguishable), if the proportion of hinders that are same in I and I is $\delta(I, I) \in [0, 1]$. Here, the pictures are almost indistinguishable substance savvy (for precedent, pictures of two unique people taken in the equivalent present, foundation, setup, and so on.). For the protected deduplication of δ-CI pictures, we apply square savvy change of the pictures and check if the two pictures coordinate square savvy, as appeared in Figure 2. The measure of the squares can shift (for example 4×4, 8×8, 16×16). We coordinate the pictures by mapping the first square of the picture with the principal square of the second picture and keep on doing this until the last square. After we convert the picture square astute, we run the DICE convention on the squares. For the hinders that coordinate, we keep just one duplicate of the square on the distributed storage.

B. Secure Deduplication of CI-images with DICE

In this segment we give a point by point perspective on the verified square dimension picture de-duplication technique dependent on the DICE convention. In the accompanying, we initially portray the framework and risk models and talk about the suspicions made in the DICE convention when connected to CI-pictures, at that point we present the adjustment of the DICE convention for CI-pictures. We call this new convention DICE-CI.

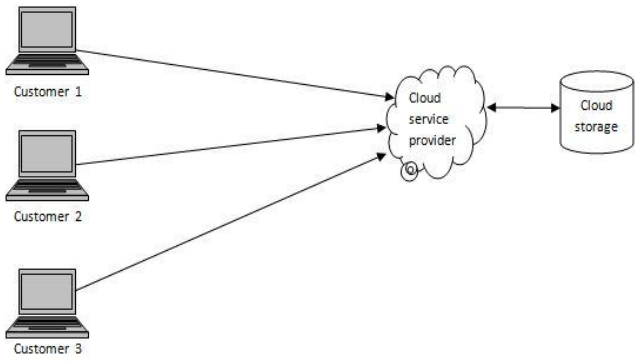

Figure 3: System overview

1) System display: The framework demonstrate is involved clients and the CSP, where there could be numerous clients getting to the cloud to transfer or download pictures, as can be found in Figure 3. CSP: The CSP gives the capacity administrations to the clients who have been allowed get to and are consequently approved to utilize the cloud administrations. For the utilization of these administrations and the capacity and support of their information, clients are charged a ostensible expense. The CSP must, thusly, guarantee the security and security of the clients'

information. Clients: Users are the general population who are approved to get to the cloud administrations. They have the scrambled record, which in this specific situation is contained a picture that they transfer to the CSP utilizing the DICE convention. Here, various clients can at the same time get to the cloud, where they convert their pictures square savvy and transfer them to the cloud. The CSP is required to keep up an entrance document that comprises of theobstructs, the ID of the picture and the client certifications. Previously transferring the picture square savvy, the customer checks for the accessibility of the squares at the cloud. In the event that a square exists, at that point a connection is given to the separate client, generally a solicitation to transfer the square is sent.

2) Threat demonstrate: In this area we think about the dangers from the part of an enemy, where they are intriguedin knowing the substance of the pictures. We consider the foe to be malignant, the CSP to be semi-vindictive and the client to be completely forthright. An enemy could be an inward or an outer foe.

An interior foe is progressively intrigued in knowing the substance of a record that may have a place with the CSP. Accordingly, we believe the CSP to be semi-fair. On the other hand, an outer foe is keen on both the content and the proprietor of the record. In this situation, the dangers could be produced by straightforwardly getting to the cloud administrations or then again by accessing the channel. In the event that the aggressor gains access to the cloud, they could attempt to eradicate the substance of the document or supplant it with an alternate record. However, independent of the goal of the foe, the conventions utilized by the CSPs ought to be sufficiently secure to ensure the discovery furthermore, counteractive action of those assaults.

3) Assumptions: We expect that the clients have been effectively validated by the CSP and conceded the important rights to get to the cloud assets. We moreover expect that the hash capacities are impact safe, and that the cryptographic natives being utilized to plan the square dimension picture de-duplication convention are secure and are computationally infeasible for any enemy to break, given adequate processing assets and power.

4) DICE-CI convention: The client first partitions the picture into a fixed number of squares. Each square size could be ofvariable length, somewhere in the range of 4×4, 8×8 to 16×16. After changing over the picture into hinders, the client runs the customer bit of the DICE convention on each square. According to the DICE convention, the customer figures the key Ki as Ki ← H(Bi) where H is the hash capacity, and Bi is the ith square of the picture. Next, the customer figures the cipher-text Ci as Ci ← E(Ki,Bi) and the label T as Ti← H(Ci), where E is the encryption system.In the wake of figuring the keys, the cipher-text and the labels, the client acquires the accompanying vector {K11,K12, ...Kmn}, {C11, C12, ...Cmn}, {T11, T12, . . . , Tmn} for a picture I, where mn is the all out number of squares. At this stage, the client sends the label vector {T11, T12, ...Tmn} to the CSP and checks for its reality in the cloud. The CSP at that point runs a scan in the label store for the presence of the labels from the label vector and sends a solicitation for just those squares for which no match was found. The customer at that point sends the cipher-text of those specific squares to the CSP, who stores them alongside the client's accreditations and updates its tag store by processing T ← H(Ci). At the season of download, the client sends the label vector what's more, user id, and the CSP looks through its label store to discover the relating tag and cipher-text obstruct as Ti = TI . On the off chance that there is a match discovered, at that point the relating cipher-text square is sent to the particular client, generally the CSP sends an affirmation that the picture isn't found. After the client gets the cipher-text, the tag is processed from the gotten cipher-text obstruct as TI = H(Ci) and is coordinated with the put away tag as Ti = TI . In the event that there is a match found, at that point the unscrambling procedure begins as Bi ←D(Ki, Ci), where D is the unscrambling technique; generally the client sends an affirmation to the CSP that the square has been ruined

Client	(a) UPLOAD	Server
$K_i \leftarrow H(B_i)$ $C_i \leftarrow E(K_i,B_i)$ $T_i \leftarrow H(C_i)$ Store K_i, T_i	$T_i \rightarrow$	$T^1 \leftarrow H(C_i)$
		If $T_i \leftarrow T_i^1$ then update U, else Request C_i
	$C_i \rightarrow$	Store C_i , $T_i^1 \leftarrow T_i$
	(b) DOWNLOAD	
	$ID_{download}$, $T_i \rightarrow$	
	$\leftarrow C_i$	If $T_i = T_i^1$ Send C_i Else $C_i$corrupt
$T_i^{11} = H(C_i)$ If $T_i = T_i^{11}$ Then $B_i = D(K_i , C_i)$ Else B_i Corrupt		

Steps of DICE-CI protocol: (a) upload (b) download

. The above convention depends on the MLE plot. There are other broadly utilized MLE based plans, for example, CE, HCE1, HCE2 and RCE, however the reason that we decided toexecute DICE based square dimension de-duplication of the pictures is on the grounds that DICE is a customer based technique which is verified against the toxin assault, not at all like HCE1, HCE2 furthermore, RCE, which are not verified against the toxic substance assault. While CE is verified against the toxic substance assault, it is a server sided methodology. In the meantime, the running time of DICE is extensively not as much as that of the CE conspire yet proportional to other customer based systems. Agarwalaet. al [3] give more subtleties on the examination and security investigation of the different MLE based plans.

IV. SECURITY ANAYLSIS

The MLE based plan portrayed above jam the protection of the information in light of the fact that the hash estimation of each square is utilized as the picture encryption key for that specific square, at that point AES is connected as the picture encryption technique. Here, the key is legitimately identified with the hash estimation of the picture square substance. Therefore, the key qualities and their relating cipher-text are exceedingly probably not going to be the equivalent, rendering it hard to discover any connection between them. This, thusly, makes it troublesome for an enemy to dispatch a lexicon assault on the square savvy encryption system. Additionally the square savvy picture de-duplication plot is secure.

Lemma 1: Block level image de-duplication is secured against poison attack.

Proof: Let us assume that the adversary computes the forged key, cipher-text and tag as K^*, $C^*$and T^*, respectively. They continue with $T^* \times Bi$ for the block B, $i \leq n$ where $T^* \times Bi = T \times Bi$. For the condition to hold true, the adversary has to compute $C^* \times B$ and make it equal to$C \times Bi$.

Figure4 :6 δ-CI image pairs$((I_1 , I_1^1) ,(I_2, I_2^1) \ldots (I_6, I_6^1))$from left to right with different values of δ.
The correspondingδ values are :
(I_1 , I_1^1)=0.53, (I_2 , I_2^1)=1, (I_3 , I_3^1)=0.02, (I_4 , I_4^1)=0.01, (I_5 , I_5^1)=0.06, (I_6 , I_6^1)=0.11

At this time, the key is related to thehash value of the image block content which results in theadversary having to ensure that $K^* \times B = K \times B$. This iscomputationally infeasible because of the one way propertyof the hash functions. Thus DICE-NI scheme is secureagainst the poison attack.

V. PERFORMANCE ANALYSIS

We approve the execution of the DICE-NI convention by running recreations performed on a system between the customer and the server utilizing Java attachments on a Windows 10 stage 64 bit with Intel Core i5. We utilized SHA256 to register the record hash and AES to scramble and decode the content.

We ran the DICE-CI convention on a 12 picture informational collection (6 picture sets) where the picture measure went from 0.019mb to 10.5mb and we limited the quantity of clients to one. The picture informational index included pictures where some have the equivalent goals yet just certain squares were extraordinary, while others have distinctive goals yet looked almost indistinguishable with slight minor departure from the squares

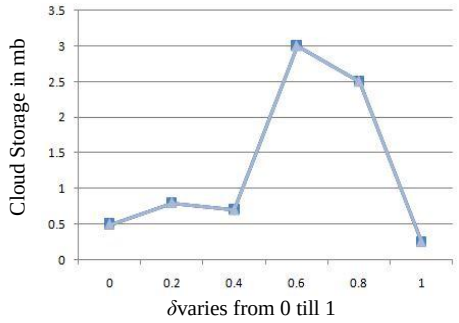

Figure 5 :Comparison of storage space at the cloud with an increasing ratio (δ) between image pairs that have similar blocks.

From Figure 5 we can see that for various estimations of δ we see a decrease in the extra room at the cloud. For instance, with δ = 0.89, the absolute extra room taken by two pictures at the cloud is 2.73mb, though the all out size of the picture pair together is 4.87mb. So also, for δ = 0.93 all out extra room required was 5.93mb. In the wake of putting away the majority of the pictures square savvy, we seen that the all out extra room for each of the 30 pictures was diminished to 17.33mb from 29.24mb, a funds of 11.91mb. We will note more varieties when there are more NI pictures transferred by various clients all the while at the CSP.

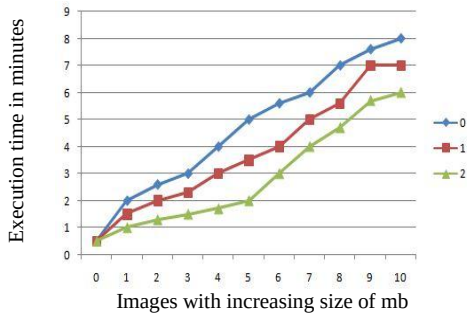

Figure 6 : Comparison of DICE-NI execution time with varying number of block size.

In the second test we run the DICE-NI plot by shifting the square size of the pictures to check the all outtime taken to execute the convention. From Figure 7 we watch the all out time taken for DICE-NI execution for pictures of changing square sizes: 4 × 4, 8 × 8 and 16 × 16.

It is obvious that the square size is legitimately relative to the execution time of DICE-NI; littler squares take more opportunity to execute than the bigger squares. Despite the fact that bigger squares take less execution time, they may prompt different issues. For instance, bigger squares could result in more information being put away at the CSP, or the clients may not have the capacity to recover the whole picture appropriately at the time of download because of the loss of some pixel esteems at the time of remaking. Albeit littler square sizes could help to accomplish better de-duplication, the labels and the keys created and put away at the customer side are of fixed size which is independent of the square size. We don't need the square size to be too little since it might overcome the entire reason for sparing extra room. With a shifting square measure, be that as it may, some almost indistinguishable pictures accomplish better de-duplication results, while different pictures don't. We watch that deciding an ideal square size with an appropriate esteem for the limit δ is a difficult assignment when running this tests.

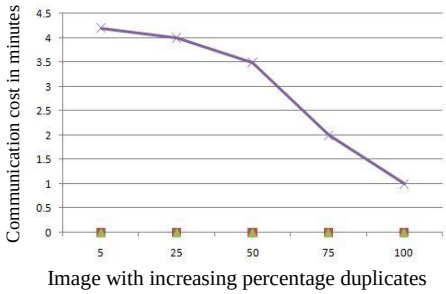

Figure 7 : Comparison of communication cost with increasing percentage of NI blocks.

In our third trial we processed the correspondence time taken by the clients to transfer and download pictures at the CSP. From Figure 8 we can watch a decrease in the complete correspondence time by expanding the level of δ, while keeping different components steady, for example, the square estimate, number of clients getting to the cloud and picture size.We might want to test this further by fluctuating every one of the parameters in request to decide an ideal capacity to lessen the generally cost.

VI. CONCLUSION AND FUTURE SCOPE

In this paper we gave a strategy to perform secure picture de-duplication at the square dimension dependent on the DICE convention. We found that the more noteworthy the comparability of the pictures, the littler the quantity of squares put away at the cloud. Notwithstanding, the requirement here was that the pictures were almost indistinguishable with little varieties among them. In the future we might want to address this issue on a more extensive range where we include more picture tasks like scaling, revolution, trimming, numerous perspectives, lighting conditions, what's more, pressure with various document organizations, and test them at the cloud

REFERENCES

[1] T. Jiang, X. Chen, Q. Wu, J. Ma, W. Susilo, and W.Lou, "*Towards efficient fully randomized message-locked encryption*", on the 21st Australasian Conference on Information Security and Privacy, Melbourne, VIC, Australia, 2016, pp. **361-375.**

[2] D. Koo, J. Hur, and H. Yoon, "*Secure and efficient deduplication over encrypted data with dynamic updates in cloud storage*," in Frontier and Innovation in Future Computing and Communication, Dordrecht, 2014, pp**. 229-235.**

[3] A. Agarwala, P. Singh, and P.K. Atrey, "*DICE: A dual integrity convergent encryption protocol for client side secure data deduplication,"* in IEEE International Conference on Systems, Man, and Cybernetics, Banff, Canada, 2017, pp.**2176-2181.**

[4] M. Bellare, S. Keelveedhi, and T. Ristenpart, "*Message locked encryption and secure deduplication*," in Advances in Cryptology- 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, 2013, pp. **296-312**.

[5] M. Bellare and S. Keelveedhi, "*Interactive message locked encryption and secure deduplication*," in Public Key Cryptography- 18th IACR International Conference on Practice and Theory in Public Key Cryptography, Gaithersburg, MD, USA, 2015, pp**. 516-538.**

[6] J. Stanek, A. Sorniotti, E. Androulaki, and L.Kencl, *"A secure data deduplication scheme for cloud storage*," in Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp**. 99-118.**

[7] M. W. Storer, K. Greenan, D. D. Long, and E. L. Miller, "*Secure data deduplication,"* in Proceedings of the 4th ACM International Workshop on Storage Security and Survivability, Fairfax, Virginia, USA, 2008, pp. **1-10.**

[8] J. R. Douceur, A. Adya, W. J. Bolosky, P. Simon, and M. Theimer, *"Reclaiming space from duplicate files in a serverless distributed file system*," in the 22nd International Conference on Distributed Computing Systems, Vienna, Austria, 2002, pp. **617-624.**

[9] K. Keonwoo, Y. Taek-Young, J. Nam-Su, and C. Ku-Young, "*Client-side deduplication to enhance security and reduce communication costs,"* ETRI Journal, vol. 39, no. 2, pp**. 116-123,2017**.

[10] H. Gang, H. Yan, and L. Xu, Secure Image Deduplication in Cloud Storage. Cham: Springer International Publishing, 2015, pp. **243-251.**

[11] F. Rashid, A. Miri, and I. Woungang, *"Secure image deduplication through image compression*," J. Inf. Secur. Appl., vol. 27, no. C, pp**. 54-64, 2016.**

[12] D. Li, C. Yang, C. Li, Q. Jiang, X. Chen, J. Ma, and J. Ren, *"A client-based secure deduplication of multimedia data,"* in IEEE International Conference on Communications, Paris, France, 2017, pp. **1-6.**

[13] X. Li, J. Li, and F. Huang, "*A secure cloud storage system supporting privacy-preserving fuzzy deduplication,"* Soft Computing, vol. 20, no. 4, pp. **1437-1448, 2016.**

[14] Ashish Agarwala, Priyanka Singh, Pradeep k, "*Client side secure image deduplication using DICE protocol*," Albony, New York, USA.

Authors Profile

Mr. Akshay R, persuing BE in Computer Science and Engineering, Department of CSE, East West Institute of Technology. And area sof interest is Cloud computing and Cryptography.

Mr. Ankith Kumar Sarawgi A K, persuing BE in Computer Science and Engineering, Department of CSE, East West Institute Of Technology. And areas of interest is Cloud computing and Information and network security.

Mr. Amith B, persuing BE in Computer Science and Engineering, Department of CSE, East West Institute of Technology. And areas of interest is Cloud computing and Data structures

Mr. Jayanth R, persuing BE in Computer Science and Engineerig, Department of CSE, East West Institute of Technology. And areas of interest is Cloud Computing and ComputerNetworks.

Prof. Kiran M, BE, MTech, Assistant Professor, Department of Computer Science and Engineering, East West Institute of Technology, has an experience of 7 years in the field of teaching, and his areas of interests are Cloud Computing, Wireless sensor networks and Internet of Things.

