International Journal of Advanced Science and Technology
Vol. 29, No. 8, (2020), pp. 6016-6024

Invertible Discrete Wavelet Transform Using Secure Data Integrity Encryption Method For Cloud Storage

Md Muntajib Uddin Faraz[1], MD. Ateeq Ur Rahman[2]

[1]Research Scholar, Dept. of Computer Science & Engineering, SCET, Hyderabad.
[2]Professor & Head, Dept. of Computer Science & Engineering, SCET, Hyderabad.
Emails:[1]farazmuntajib@gmail.com,[2]ateeq@yahoo.com

Abstract

Protection on end customers' data set aside in Cloud workers transforms into a huge issue in the current Cloud conditions. In this paper, we present a novel data protection procedure uniting Selective Encryption (SE) thought with brokenness and dispersing on limit. Our method relies upon the invertible Discrete Wavelet Transform (DWT) to segment freethinker data into three areas with three particular degrees of protection. By then, these three segments can be dissipated over different amassing areas with different degrees of steadfastness to guarantee end customers' data by contradicting possible openings in Clouds. Along these lines, our strategy upgrades the limit cost by saving expensive, private, and secure additional rooms and utilizing unassuming anyway low reliable additional room. We have genuine security assessment performed to check the high protection level of our methodology. Likewise, the efficiency is exhibited by execution of sending tasks among CPU and General-Purpose Graphic Processing Unit (GP-GPU) in a smoothed-out way

1. Introduction

With both the improvement of PCs and Cloud enlisting development, the example starting late is to redistribute information gathering and dealing with on Cloud-based organizations [1]. The Cloud-based organizations for solitary end customers [2] are getting commonness especially for data storing. Contingent upon colossal additional room and strong correspondence channel, Cloud-based expert associations, for instance, Dropbox, Google Drive, or Amazon Drive just to give a few models, are giving individual customers essentially boundless and insignificant exertion additional room. This condition raises the issue of the steadfastness of Cloud master associations. Various data security and insurance scenes are found in today's Cloud organizations [3], [4], [5], [6]. From one perspective, Cloud expert associations deal with a huge number of outside ambushes. In 2018, an aggregate of 1.5 million SingHealth patient's non-therapeutic individual data were taken from the prosperity structure in Singapore. Then again, Cloud authority centers can't be totally trusted either [8]. Singular data may be manhandled in a malevolent course, for instance, in the Facebook and Cambridge Analytica data humiliation which affected 87 million customers in 2018. Subsequently, it ends up being dynamically noteworthy for end customers to capably guarantee their data (works, pictures, or accounts) openly from Cloud authority communities. One reasonable course of action is to guarantee data on a protected end customer's machine before re-appropriating to Clouds which ordinarily becomes standard figures, for instance, AES. In any case, encryption figuring's are moving security on data to affirmation on keys which in this way, presents key organization issues. At the point when the key is revealed, data security will be undermined. All the more terrible, if the end customers have no cryptography incredible practice and endeavor to reuse a comparative key for different data confirmation, one key presentation will provoke a tremendous extent of data spillage. In like manner, despite figures, other data security plans are critical to support such circumstances. One past research course is the Selective Encryption (SE) [11] which is normally seen as lightweight encryption strategies dedicated for sight and sound data positions. They abuse redundancies of blended media data and are generally considering weight computations. Generally, they discrete data into two segments. A private piece contains most of the information, with the ultimate objective that this area is commonly sufficient to fathom the main data. A consequent piece, called open piece, must to contain a much humbler proportion of information while taking a huge additional room. These two

ISSN: 2005-4238 IJAST

pieces are explicitly verified with different methodologies as demonstrated by their different order levels. SE methods' state of craftsmanship shows that each SE system is planned to verify a specific kind of media data and information mishap are unavoidable.

2. Related work

In this area, we will quickly present the current SE techniques and point out the weaknesses. Some new criteria will be additionally referenced to think about our outcomes and existing arrangements. In [15], the most two basic criteria for the media SE techniques are appeared as histogram investigation and relationship investigation. In any case, the criteria for assessing information security techniques ought to be reached out as indicated by the down to earth use cases, for example, the safe information stockpiling from the end clients to Clouds portrayed in this paper. For example, the execution speed must be estimated on down to earth equipment stages and contrasted and encryption calculations (AES-128 in this paper). The security level must be too assessed by the plan reason. Information honesty, as an essential prerequisite for acknowledging group skeptic, is additionally critical to be assessed. For the protected information stockpiling from end clients to Clouds use case, thinking about the capacity designation improvement and protection from blunder spread are additionally fundamental. The concise correlation is appeared in Table 1. For assessing the execution speed, it is essential to first think about whether in the structure level there are extra preprocessing steps, for example, the DCT procedure appeared in [18]. For this technique, just the preprocessing step dependent on DCT is slower than utilizing AES on the whole information found on a current CPU as pointed in [15], prompting execution issues that are not mulled over. Such issue is continuously overlooked by change based SE strategy, for example, [19], [20], [21]. In our technique, we use GPGPUs to accelerate the estimation assignments and the execution times are assessed to demonstrate the productivity contrasted and AES or AES-NI. The security level is constantly founded on the plan reason. For example, some sight and sound SE strategies are intended to just decrease the special visualizations which are ordinarily observed as low-level considering security, for example, [18]. All the more explicitly, in the event that the insurance is just done on the private parts, we consider it as low security level as there are many related attempts to show the immediate recuperation from general society pieces for example, [13], [22]. In this manner, the main past works qualified high security levels in Table 1 are [15], [21], [23]. In this paper, serious security investigation is performed to demonstrate a high security level is accomplished with ensuring both the private sections and open parts. Information uprightness is a significant criterion however is consistently disregarded in past SE techniques. For example, in [20], a partial Wavelet-based SE technique is utilized to corrupt the picture quality. Be that as it may, information trustworthiness can't be ensured as the adjusting blunders of estimations among whole numbers and drifting point numbers are overlooked which will cause genuine issues as appeared in [22]. For the SEstrategies dependent on pressure and coding, the information respectability could be ensured. Notwithstanding, SE techniques structured dependent on pressure furthermore, coding procedures are continually depending on the subtleties of explicit pressure and coding calculations which lead to blunder causing and group dependence. For example, in [23], a security strategy for JPEG2000 pictures is introduced comprising in permuting the MQ query table. This will lead to blunder spread in the deciphering procedure when there are minor blunders in the transmission and furthermore make this strategy just accessible when MQ coding is utilized. Such issue is stayed away from in our strategy with preparing information as frameworks of bytes in a freethinker way and planning the distribution of information pieces as per correspondence channel status. Capacity advancement is considered in this exceptional use instance of secure stockpiling from end clients to Clouds. For most SE techniques, the discontinuity idea isn't structured based on the capacity utilization of open Clouds which enhance the extra room use of the confided in zone. In this short audit, just the work appeared in [15], [23], [24] could be utilized to streamline the believed stockpiling region by transferring people in general pieces to the Clouds. In this paper, we characterized the classified levels of the pieces and people in general sections are additionally secured. In this way, the little private part with high classified level can be put away in a zone trusted by the end clients while the general population and ensured pieces can be put away on open Clouds with protection from assaults.

ISSN: 2005-4238 IJAST

3. Design and implementations

In this segment, we initially present the general idea of particular encryption and afterward consolidate it with the thought of fracture and scattering. Thereafter, a few key structure and usage components will be given all together to represent with our pragmatic insurance strategy.

3.1 General Concept

The underlying thought of existing SE strategies is to secure a piece of data by scrambling just a piece of it. This could increment the general execution for interactive media substance by decreasing the information sum that must be encoded. In our plan, extra ideas are presented: discontinuity furthermore, scattering. As appeared in Figure 1, input information d is isolated into two sections, d1 and d2: d1 must take significant components of unique data and little stockpiling space. d1 will turn into the private section after encryption. d2 is the general population part. It is planned to take up the vast majority of the extra room, while conveying minimal relevant data from d. At that point, d1 can be put away in nearby and private stockpiling which could have restricted extra room and d2 can be put away in an open Cloud with lightweight security.

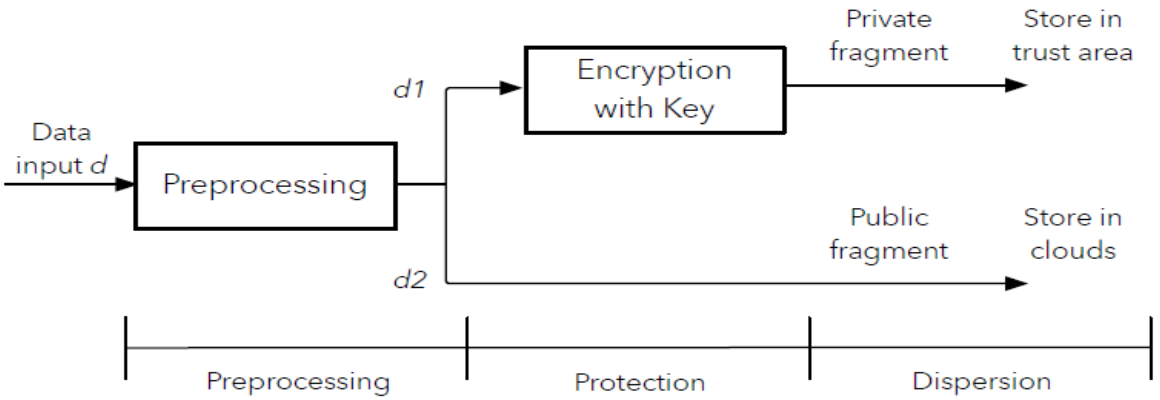


Figure 1: Concept of SE with a dispersion into two independent locations optimizing trust area storage usage.

3.2 Discrete Wavelet Transform

In past works [18], [29], Discrete Cosine Transform (DCT) was utilized to help fracture choice previously performing SE for bitmap assurance. As called attention to in [15], DCT can't ensure the loss lessness because of changes among whole numbers and drifting point numbers which will bring about adjusting blunders [22]. These adjusting blunders can be decreased with an exact plan with more extra room, however can't be completely dodged. This issue makes DCT unusable what's more, unfit to give the essentially required honesty in request to manage information positions. DWT is a sign preparing strategy used to remove data that is generally utilized in interactive media pressure standard, for example, JPEG2000. It can speak to information by a set of course and detail esteems in various scales. Normally, it is a one-dimensional change, yet it can likewise be utilized as a two-dimensional change applied in both the level also, vertical headings. For the two-dimensional case, DWT will create four sub-frameworks where each sub-lattice is a quarter size of the first grid. Results for one level 2D-DWT are: unified with low goals (LL), one with high vertical goals and low-level goals (HL), one with low vertical goals and high-level goals (LH), and one with all high goals (HH). At that point, the second level change might be accomplished for the LL part which is called dyadic decay as appeared in Figure 2. In our plan, a two-level 2D-DWT is picked and is represented in Figure 2. The Le Gall 5/3 channel [30] is being utilized as it has a significant lossless property. The DWT- 2D dependent on Le Gall 5/3 channel fits best for our plan by giving the two-information propriety and productivity as it can appreciate the speeding up brought by GPGPUs [16], [31]. The chose coefficients utilized so as to manufacture the private section are the second LL which takes

ISSN: 2005-4238 IJAST

around 1/16 of the extra room and conveys the fundamental components (coarse data) of the information lattice. The explanation behind utilizing two-level DWT is that the one level DWT still has an enormous section (1/4 of the entire DWT-2D consequence) of LL coefficients so as to have the option to ensure, and at least three DWT levels so as to make the range esteem of the high recurrence coefficients excessively huge, prompting the pointless utilization of extra room. Execution of DWT must be viewed as dependent on opposing the execution time against full encryption. In a few situations, the preprocessing steps of SE can genuinely be disregarded, as SE and pressure are incorporated, such change is being utilized by the two applications [32]. Be that as it may, our utilization case that includes any sort of information, will have to consider the whole procedure with regards to execution assessment. This will lead us to actualize DWT on a GPGPU so as to profit by the speeding up provided by the parallel engineering of a GPGPU [33] (more usage subtleties in Section 5).

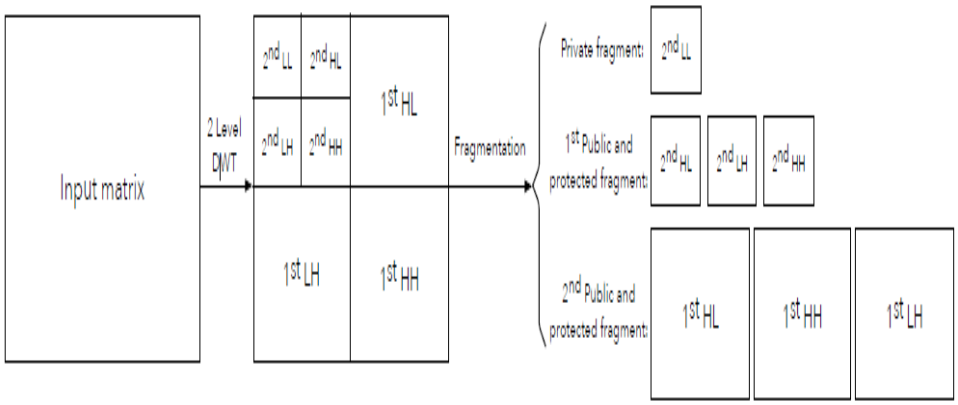


Figure 2: An example for a two-level DWT which generates two-dimensional coarse and detailed values.

3.3 System Designs

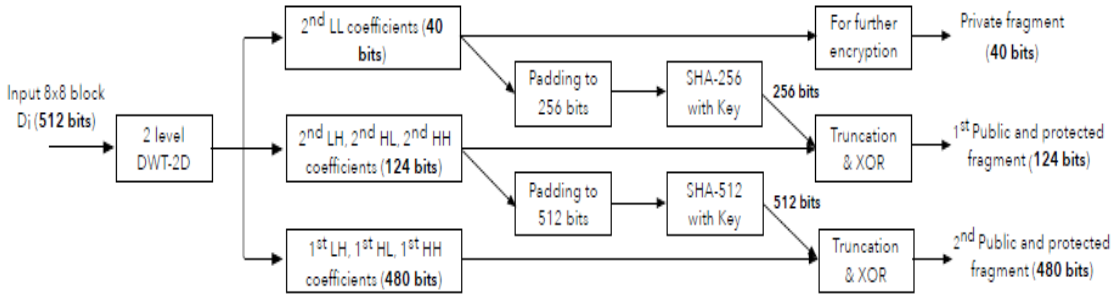
Any sort of information can be viewed as an arrangement of information pieces Di were each lump Di will be characterized thus as a square network with a tunable size (512512 or 10241024 bytes), contingent upon the settlement of change or the equipment execution. Each component of Di is a byte which can be viewed as an 8-piece whole number. At that point each piece Di will essentially be handled utilizing the SE strategy obstruct by obstruct with a square size of 8x8 as appeared in Figure 3. The lump size can be changed by the usage subtleties, particularly the GPGPU equipment setup. The square size should be constantly 88, which fits best our configuration as showed in Section 3.4. This tiling step is utilized not just for fitting with the GPGPU design yet additionally for the best plan of the three pieces in Figure 3. For each 8x8 square, the initial step is to play out the 2D Discrete Wavelet Transform (DWT-2D). In our work, two progressive degrees of the DWT-2D were performed with the Le Gall 5/3 channel. The low recurrence coefficients (2ndLL coefficients) are considered as the private piece. This part removes just 4 from 64 coefficients however conveys most of the data as per a vitality perspective. The AES-128 piece [10] will be utilized to secure this part. In our plan, the code is organized with the end goal that another figure calculation can without much of a stretch supplant AES-128 if necessary. The other two coefficients levels are considered as the two "open and ensured parts" (PPFs) as appeared in Figure 2. The private piece of every 8x8 square will at that point be utilized to produce a 256-piece grouping, by utilizing SHA- 256 [34]. This will ensure the age of various piece groupings, in any event, when the relating private parts in the neighboring squares are fundamentally the same as (encryption key is additionally included to ensure the key affectability as appeared in Figure 3). This bit grouping is utilized to ensure the first PPFs (the rest of the coefficients of second level DWT are appeared in Figure 2) by playing out a XOR activity. This piece is characterized as the first PPF. For the second PPF which contains the remaining DWT coefficients, insurance is finished by XORing it with a piece succession created from SHA-512 [34] based on the contributions of first PPF and the encryption key. The assurance of the PPFs is given by

ISSN: 2005-4238 IJAST

XOR activities furthermore, depends on the irregularity ensured by the SHA capacities. For instance, at times like bitmaps, as long as there are redundancies because of comparative neighboring pixels, the recurrence coefficients could be fundamentally the same as, particularly between neighbor squares. Nonetheless, the SHA- 256 and SHA-512 capacity will produce an entirely unexpected bit succession, in any event, when there is just a single distinctive piece as input (for example 2ndHL as contribution for SHA-256; 2ndHL, 2ndLH what's more, 2ndHH as contribution for SHA-512). This irregularity will at that point be added to the PPF by XORing comparable recurrence coefficients along arbitrary hash estimations of the last layer of the parts. Moreover, this plan additionally has a decent impact to oppose against redundancies of any sort of information records. Greater security investigation will be appeared in Section 4. For the defragmentation and decoding, it is easy to simply turn around the procedure in Figure 3 since all means are symmetric.

3.4 Numerical Precision to Enable Agnostism

The preprocessing step used to isolate information may prompt honesty issues, where information when switching insurance could be extraordinary. In past SE techniques, this is ordinarily because of adjusting mistakes of changes between whole numbers and gliding point numbers. One approach to explain this issue is portrayed in [35], where the creators proposed to announce all factors with a twofold accuracy dependent on their bit-length of 64 bits. This prompts an enormous increment in the use of extra room without having the option to thoroughly stay away from such adjusting blunders. In any case, it isn't ideal in wording of impressions to utilize bigger extra room so as to drift accuracy numbers, particularly if the information is put away as a whole number with a piece length of 8 bits, where the subsequent extra room will require multiple times the extra room of the unique information. In [15] an enhanced worth portrayal in terms of the impression was structured, yet it was unrealistic to absolutely abstain from adjusting mistakes brought about by the DCT. In this paper, the preprocessing step is the DWT based on "LeGall 5/3" channel which is intended to be a whole number to integer map, to such an extent that this DWT is lossless. Thus, on one hand, any adjusting blunder is kept away from; then again, the additional extra room use brought about by the int to glide change doesn't exist either. The main conceivable extra capacity use can be brought about by the diverse range esteem of the info 8-piece int, and the yield int coefficients. The yield esteem range can be determined as long as the info values are constantly put away Byte by Byte. The info esteem run (seen as unsigned worth) will be then from 0 to 255 which can be considered as from −128 to +127 (the range is viewed as from −128 to +128 during the accompanying figuring). At that point the capacity strategies can be planned by the worth go appropriation. The primary level DWT-2D change is really determined by twice DWT-1D changes on the 8*8 hinder in flat and vertical ways successively. The first even change produces two sub-grids which are 1stL and 1stH that take every 50% of the outcome grid on a level plane. The vertical change is done on every one of the two sub-grids which creates four sub-matrices like in Figure 2 (1stLL; 1stHL; 1stLH; 1stHH). In the principal even change, the range for 1stH is - 255 to +255 (did twofold the info extend), and the range for the 1stL is - 192 to +192 (increased the info run by 1.5 occasions). At that point the change in the vertical heading, which changed the 1stL and 1stH squares individually, gets the accompanying outcomes: 1stHH is from -511 to +511 what's more, the range for 1stLH is from -384 to +384.



ISSN: 2005-4238 IJAST

Figure 3: Proposed SE method for the single 8*8 block

All the coefficients in the three sub-networks of the principal level of DWT-2D changes can be put away utilizing by 10-bits space. The worth scope of second level DWT-2D coefficients is produced by a similar two bearings DWT-1D that changes the 1stLL sub-frameworks coefficients. The range of the second level DWT coefficients can be assessed by streamlining the conditions of DWT-2D with "LeGall 5/3" channel, and afterward straightforwardly get comes about because of ascertaining the last recipe of every component in the four sub-frameworks in Figure 2 (2ndLL; 2ndHL; 2ndLH; 2ndHH). Also, the maximum qualities and min esteems for every one of the worth evaluated are appeared in the accompanying lattices. The capacity technique for the second level DWT-2D coefficients is: 11-bits for every one of the lower left corners, four coefficients (2ndHH), and 10-bits for remaining of the coefficients.

$$\begin{bmatrix} 338 & 260 & 468 & 468 \\ 260 & 200 & 360 & 360 \\ 468 & 360 & 648 & 648 \\ 468 & 360 & 648 & 648 \end{bmatrix} \begin{bmatrix} -338 & -260 & -468 & -468 \\ -260 & -200 & -360 & -360 \\ -468 & -360 & -648 & -648 \\ -468 & -360 & -648 & -648 \end{bmatrix}$$

3.5 Storage Space Usage

As brought up in Figure 3, the private part that we chose is a sub-grid (2ndLL of Figure 2). As indicated by the structure, this private piece should be put away in a confided zone (locally in this paper), and the remaining two pieces should be put away out in the open Cloud servers. Truth be told, this stockpiling setup for the three sections could be adaptable as per the nature of the correspondence channel. The extra room taken by the private section will be just 7:8% of the information size (for each square, just 40 bits contrasted and the first extra room 512 bits). Be that as it may, if the transmission mistakes are considered, the torrential slide impact [36] must be evaded. In such a circumstance, the first PPF will likewise be put away in a trusted region with the private part. This plan is additionally picked as the one assessed by us for the extra room plan in this paper. The pieces put away locally will take 164 bits altogether (40 bits for private piece and 124 bits for the first PPF as appeared in Figure 3). The piece scattered to the Cloud servers will take 480 bits. The all-out extra room utilization is 644 bits, in any event which is about 26% more than preliminary information 512 bits, however the second PPF (480 bits) can be put away on Clouds without spills, and the private part is all things considered 32% as per the more grounded stockpiling plan. In rundown, the preprocessing step is the DWT-2D based on "Le-Gall 5/3" channel which is intended to be a whole number to integer map is lossless. In our plan, we think about any sort of information type as int with bit-length of 8 bits which implies notwithstanding the kind of unique information, we read the information by taking each byte in turn and perusing it as an 8-piece whole number. At that point, the information bytes will shape a 2D grid of a configurable size. Therefore, on one hand, any adjusting mistake can be maintained a strategic distance from; then again, the additional extra room utilization that could be brought about by the int to skim transformation doesn't exist. Likewise, the numerical information kind of factors associated with DWT calculation is deliberately structured, in a way that can give the lossless property, in this way giving essential skepticism for any information groups.

4. Proposed algorithm

Fragmentation + Encryption + Dispersion (FED algorithm)

Definition

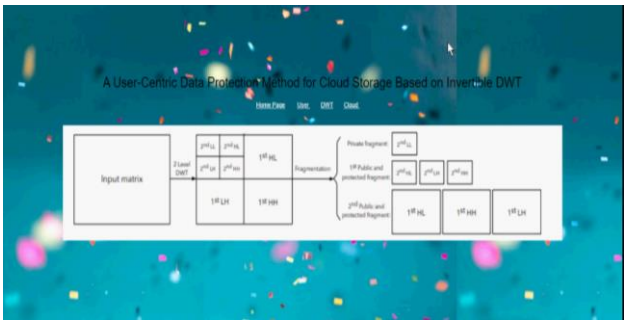
We have proposed an algorithm to introduce an accelerator for better performance which combines Fragmentation + Encryption + Dispersion. Our FED algorithm can see as an extending the classical SE concept by designing a novel data protection scheme supporting data integrity. We can see our

ISSN: 2005-4238 IJAST

proposed method in a cost-effective storage manner with an end user to cloud scenario which can protect data against different threats.

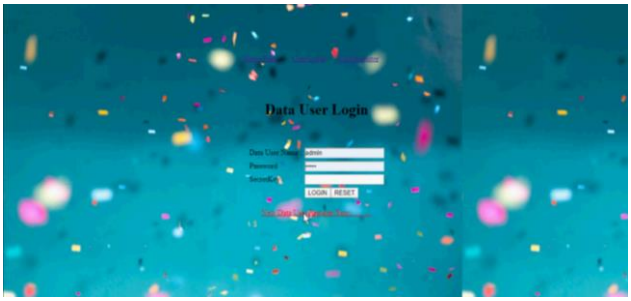
5. Result

This below screen will get when we execute our project.



This page screen is for new user registration.

Once the user gets register then in this all the existing users will perform login operations.



Once the user has successfully registered then he will get redirected to his home screen.

ISSN: 2005-4238 IJAST

In this screen user can search the file by entering that file name.

6. Conclusion

In this paper, we proposed an answer for end clients to misuse the utilization of modest Cloud stockpiling administrations while keeping their information safe. Our technique can be applied on a wide range of information designs which altogether improved the idea of specific encryption by presenting discontinuity and scattering strategies. The trial and hypothetical outcomes have confirmed that our technique can give a significant level of security with opposition against causing blunders. We additionally gave a quick runtime on various PC stages with commonsense structures and usage dependent on GPGPU increasing speed. In outline, we proposed a safe and proficient information insurance technique for end clients to safely store the information on Clouds.

References

[1] F. Hu, M. Qiu, J. Li, T. Grant, D. Taylor, S. McCaleb, L. Butler, and R. Hamner, "A review on cloud computing: Design challenges in architecture and security," Journal of computing and information technology, vol. 19, no. 1, pp. 25–55, 2011.

[2] H. Li, K. Ota, and M. Dong, "Virtual network recognition and optimization in SDN-enabled cloud environment," IEEE Transactions on Cloud Computing, 2018.

[3] Y. Li, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," IEEE Transactions on Computers, vol. 65, no. 5, pp. 1339–1350, 2016.

[4] L. Kuang, L. Yang, J. Feng, and M. Dong, "Secure tensor decomposition using fully homomorphic encryption scheme," IEEE Transactions on Cloud Computing, 2015.

[5] J. Wu, M. Dong, K. Ota, J. Li, and Z. Guan, "Big data analysis based secure cluster management for optimized control plane in software-defined networks," IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 27–38, 2018.

[6] K. Gai, K.-K. R. Choo, M. Qiu, and L. Zhu, "Privacy-preserving content-oriented wireless communication in Internet-of-Things," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3059–3067, 2018.

[7] S. Hambleton et al., "A glimpse of 21st century care," Australian Journal of General Practice, vol. 47, no. 10, pp. 670–673, 2018.

[8] K. Gai and M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers," IEEE Transactions on Industrial Informatics, 2017.

[9] O. Solon and O. Laughland, "Cambridge analytica closing after Facebook data harvesting scandal," The Guardian, 2018.

[10] W. Dai, "Crypto++ library," 2007.

[11] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, and J.-J. Quisquater, "Overview on selective encryption of image and video: challenges and perspectives," EURASIP Journal on Information Security, vol. 2008, no. 1, p. 1, 2008.

ISSN: 2005-4238 IJAST

[12] T. Xiang, J. Hu, and J. Sun, "Outsourcing chaotic selective image encryption to the cloud with steganography," Digital Signal Processing, vol. 43, pp. 28–37, 2015.

[13] H. Qiu, G. Memmi, X. Chen, and J. Xiong, "DC co-efficient recovery for JPEG images in ubiquitous communication systems," Future Generation Computer Systems, 2019.

[14] G. O. Karame, C. Soriente, K. Lichota, and S. Capkun, "Securing cloud data under key exposure," IEEE Transactions on Cloud Computing,2017.

ISSN: 2005-4238 IJAST