# A SURVEY ON CRYPTOGRAPHIC ALGORITHM FOR DATA SECURITY IN CLOUD STORAGE ENVIRONMENT

[1] B.UMAPATHY
*Research Scholar Dept. of Computer Science College of Science and Humanities SRM Institute of Science and Technology Kattankulathur Chennai*

[2] DR. G. KALPANA
*Associate Professor & Head Dept. of Computer Science College of Science and Humanities SRM Institute of Science and Technology Kattankulathur Chennai*

***Abstract***
***People are using lot of cloud storage service (CSs) to store documents. The cloud storage services are used to conserve people personal data and facilitate data transferable. The computer which connected via internet is adequate to access the data anywhere without carrying any physical drives like Pen drive, CD, etc. In existing techniques like, CSs providers are using 256-bit Advanced Encryption Standard (AES) and 128-bit (AES) encryption algorithm. This is one of the best techniques to secure data, but once the intruder gets encrypted data, there is possibility for data insecurity by means of applying brute force attacking technique in future increasing the speed performance of computer. The objective of this paper to analysis cryptographic algorithm which perfume on various data formats and data security attacks and threads in cloud storage environment. The aim to overcome this kind of attacks and key tampering technique, the key generation and maintain process handover to user's itself. It makes cloud storage service provider to maintain data only, with high efficient encryption technique that provides strong protection for data.***

***KEYWORDS: cloud storage services, cryptography, security, multifactor authentication***

## 1. INTRODUCTION TO CLOUD COMPUTING IN DATA SECURITY

In cloud storage and computing environment data privacy and its security are the major concern. To overcome this concern, we fuse cryptography concepts into cloud computing. Cryptography help in data encryption and decryption procedure is use to protect the data in cloud. To ensure privacy, data encryption is done by the user. The user share the file through cloud but person who knows the key only can decrypts the file [21]. The intruder get the file but they can’t decrypt. In evolution process, intruder try to crack the key using look up table technique, brute force technique etc.

The traditional security methods are not masterly enough to manage the cloud specific threats. The enhancement of the key building concepts which plays vital role in data security in cloud computing. By generating type of keys are public key and private key [32]. In later part technology developed and advance concepts make the encryption process with hashing techniques. Using hashing techniques the key was hashed with salt, now users itself don’t the key after the hashing. On go through process user enter the key for decrypting the file. Initiation decryption, first key was hashed with salt in background process. The output of hashed key will be executed in the decryption process. Finally, the evolution process of encryption algorithm: algorithm itself generate the round keys in fusion of master key which given by the user. These techniques are used to secure data in cloud environment.

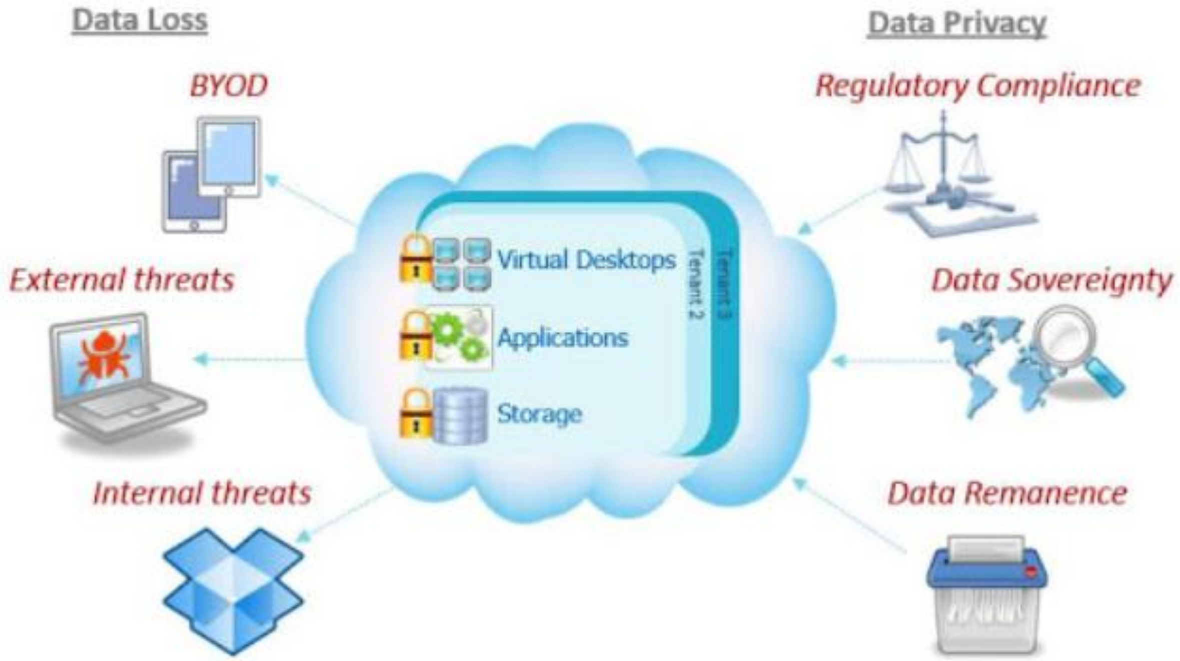

FIGURE 1: Cloud storage data security threads

In above figure illustrating that what are the threads and issues are facing by the cloud storage. Here clearly defining the internal threats, external threats, shared technology vulnerability, etc. that says whatever the data stockpile in cloud storage by people is already in high risk state [31].

This paper is summarized follows through as: In Section 2, literature review for cloud data security. In Section 3, the comparison of methodology with defining problem, implication, merits and demerits. In Section 4, concluded the summarization of whole paper.

## 2. LITERATURE REVIEW FOR CLOUD DATA SECURITY

S. Atiewi et al., (2020) abstracted an IOT based multifactor authentication and light weight cryptography encryption scheme in cloud storage environment. IOT device are organize as follow of sensitive data and non-sensitive data. The sensitive data is split in two and each part encrypted by separated encryption algorithms (RC6, Fiestel) and data deposit on private cloud storage to ensure the high security. Non-sensitive data is encrypted by single algorithm (AES) as stored in the public cloud. Multifactor authentication ensure through the trusted authority. Using the identification of user's such as IP, password and biometricsin [1].X. Wang and Y. Su (2020) proposed a new encryption method for audio which dispense reliability state high. Preliminary value that presents in chaotic controlled by hash value on the audio and then making unpredictable chaotic trajectory, DNA coding is used tomystifying and scatter the data (audio). Encryption scheme is used for single and dual format audio [2].D. Changet al., (2020) illustrated a cancelable multi-biometric approach by fusion of fuzzy extractor with a novel bit-wise encryption scheme to engender cancelable biometric templates. The protection scheme for bio-metric template framed as irreversibility, renewability and accurate recognition of biometric scenes. The scheme that safeguard without supplementary noise that means of bit errors is executed in preserved template [3].

F. Shahidet al., (2020) stated new scheme for data Security with less complexity. Proficient security our distributed storage concept divided the data as sensitive along with normal part. The data specified as normal, separately encrypted after saved insingle storage cloud but the sensitive in seriated asdual portion, the encryption process done separately and stored in different cloud. This proposed method is used to secure against following attack, related key attack, man-in middle attack, pollution attackin [4].

J. Zheng and L. Liu (2020) proposed 2D chaotic system is fusion of sine mapsalong withlogistic map. The sine map makes on combination of two chaotic maps. Now, new encryption design for a dynamic DNA encoding and decoding. Using this algorithm achieved security test, they are key sensitive, histogram and correlation analysis. It makes difficult for most successful attacks in [5]. Y. Zhang and B. Li (2020) conducted neuron-like scheme, masking operation, flipping operation for image cryptographic algorithm. The neuron-like based learning scheme makes to identify a catchy scattered scheme and execute the plaintext based image encryption algorithm. The process gets input and weights of the neuron through the feedback operation to regulate the information of image. Finally, the encryption algorithm which makes to scatter the image data. It results high security and adaptive characteristicsin [6].

H. Hu, et al., (2019) Identified intruder can intrude any important information on mode of transfer. To rectify an issues by encryption process done before the transmit data for cloud storage. For protection of hidden encryption password, designed hidden transmit mode along with multi authority factor. First user split a hidden password which makes encrypt important file splits trivial parts. Then user use the own key along with biometrics to conceal a hidden password parts [7].Y. Song et al., (2019) evolved novel based key substitution encryption algorithm purpose a progressing key for upgrade the commencing keys implement plain image and evolve another substitution scheme that encrypting different category images. It helps to overcome the low security and low computational that apply uses single round encryption only. The proposed substitution method which establish on s-boxes to different categories image encryption [8].W. I. Khedr et al.,(2019) CAPDP allows storage user to do data integrity verification infinite. The verification process is self-reliant of the count of blocks being checked in [9]. W. Feng, et al., (2019) [10] enhance the hash value which used in the plain image during encryption activity makes unworkable for intruder to deploy of special plain-image attack. DNA encoding and decoding schemes invoke plain image correlated DNA order progress further dependent on hashed data.

H. T. Poon and A. Miri (2019) abstracted technique used phrase search based Bloom filters in [11]. It uses services of n-gram filters to adopt functionality. It allows phrase search to execute self-sustain without initial progression of conjunctive keyword based search that detect user files. H. Lin (2019) discusses pre-authentication and post authentication of user to avoid anonymity. In this scheme administrator assist the user to generate the pseudo identity which is known to the user. Using the pseudo identity administrator registering in cloud servers and it help to verify user’s authentication of requesting client. This technique is very useful trace the illegal user. This protection support fast error detection or offline password update [12].

A. A. Pammu et al., (2019) Proposed matrix transformation based on authentication and parallel encryption implemented on multi-core processor. It helps to active high through put, comprehension performance and secure AES construct on counter with chaining mode [13]. W. Luo et al., (2019) Introduced new password protect which desires from plaintext password to hashing password, hashing password, to negative password and finally using symmetric-key algorithm for creation encrypted negative password. They conclude technique is secure from lookup table attack as dictionary attacks [14].

Q. Zhang et al., (2019) presented algorithm used image hashed data to frequentative progressing aspect of matrix to enhance parameterized value of chaotic maps, it increases the association of key along with original image. The generation of any-order by chen’s chaotic structure is processed for any-order encryption process the DNA coding and decoding process.

Finally, they achieve solution for problem of counter statistical attacks, noise attack and robustness of cropping, plaintext sensitivity and differential attacks at [15].

H. Tang et al., (2018) proposed three layered dynamic encryption process depend upon DES along with network coding. The encryption process depends on the partial key update work done in low complexity and which strengthen the adaptability of different cyber conditions in [16].J. Howe et al., (2018) address that Asymmetric cryptography is required large amount of computation and storage. The elliptic curve cryptography is used to decreases power consumption, increases devices performance and it have strong enforcement to conform secure communication especially when the message is encoding in elliptic curve. Proposed the Secure and Efficient Encoding scheme to address the encoding part, eventually important to secure the mapping of the message and it benefits by resisting to several attacks [17].

Y. Liu, Q. Zhong et al., (2017) designed user dependent data backup scheme using multifactor authentication. User using a symmetrical key and divided it into three shares. Finally delete the key. To access the data, key can reconstruct easily by combining the shares in user’s smart card, pen drive, laptop etc. For laptop and smart card lost or damage they use, the password and biometric for recovery process [18].Y. Zhang et al., (2017) proposed scheme to work or reinforce batch validation along with process of data dynamic operation. In proposed method audition at most required to evaluate message validity code tag for validation. It is self-sustained with number of validation works. This method attain light weight verification in auditor side [19]. K. Bai and C. Wu (2016) stated AES like Cipher, protecting encryption key during the execution of the AES algorithm in open sources devices. It is depend upon key-relaying S-boxes key expansion. S-boxes works as a key expansion and these S-boxes is applied to all the round keys. The S-boxes is used to preventing the known white-box attacks [20].

J. K. Liuet al., (2016) discusses two factor authentication for data safety prospection process with aspect volatile cloud storage environment. Here encrypted data transfer through the cloud from sender to receiver but decryption process is done by two keys, first is secret key and another one is unique key. When both key are valid only the decryption process executes [21].H. D. Nguyen and K. Turitsyn (2016) stated the judgment a small- signed stability of operating points with new proposed novel mathematical “robust stability” criterion. It helps to provides mathematical promise stability of the operation point at any multiple connection of the loads. RSA prosper to confirm the solidity the ability without making any speculation on the multiple response for load [22].

C. J. Mitchell (2016) criticized the van oorstch-wiener attack which is executed with both cipher text and plaintext sets produce utilizing a variety keys. They suggest 80 bits of security key is better than 56 bits of securities. The objectives are identified in [23].The key change in regular interval helps to limits the impact of successful attacks but it don’t minimal the attack’s triumph possibility [24].F. Guoet al., (2016) introduced new encryption notion and its construct such a distance driven encryption for the internal outcome encryption which is admissible for size of private key and cipher texts. Here the new encryption notion works, In encryption phase biometric scanned a private key to get encrypted cipher ,in key generation phase with another biometric scanned private key can decode a encrypt key. When the algorithm realize that two biometric transits that identical [25].

J. Hong et al., (2015) analyze DAC-MACS is handling the attribute repudiation the main constructing progress has certify safe. The excluded user are allowed acquire unapproved file, the attack algorithm wants conversion cipher-text existing-version to older-version. Excluded user can manipulate the cloud storage provider obtain adequate cipher test upgraded keys. This bugs will be prevented effectively in DAC-MACS scheme [25]. Artificial intelligent techniques are developed in [26] P. Roberto de Oliveira et al., (2014) quoted that energy consumption between the key generation of ECC Algorithm and RSA algorithm. Cryptographic keys are used to the authenticate procedures within entities broadcasting that improve safety of transfer. They tested the feasible connection within energy utilization along with runtime process. Finally concluded that the ECC algorithm stated low energy utilization than the RSA algorithm [27].

J. Niet al., (2014) proposed most effective multiple verifying protocol transaction depend upon distributed along with parallel system. They manifest protocol are timid, some active adversary is penetrable in cloud storage. Auditor can detected arbitrarily modified cloud data in auditing process [28].L. Zhouet al., (2013) Proposed method which incorporate cryptographic concepts, where pole based access control is named as role based encryption (RBE), they presents a safe RBE-based combination of cloud storage environment permit a concern to save records assumed on public storage and storing confidential data in private cloud storage [28]. Problem formulation is discussed in [29].

## 3. COMPARISIONS OF METHODOLOGY

**TABLE 1. Comparison of methodology**

| Sl. NO | METHODOLOGY | PROBLEM DEFINITION | IMPLICATION | MERITS | DEMERITS |
|---|---|---|---|---|---|
| 1 | Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography | In current cloud integrated IoT clearly suffer by limitations in secure authentication and encryption schemes | The classification of sensitive and Non-sensitive data helps to uses separate encryption scheme for different file type along with | The sensitive data are more secured then existing encryption technique | Trusted authority plays major role in multifactor authentication that allows the trusted authority to manipulate the data or owner ship |

| | | | | | |
|---|---|---|---|---|---|
| | | | different cloud storage to secure the data with multifactor authentication | | |
| 2 | Audio Encryption Algorithm Based on DNA Coding and Chaotic System | In audio encryption process DNA coding confess having problems they are high association and encryption speed become slow | Preliminary value that presents in chaotic controlled by hash value on the audio and then making unpredictable chaotic trajectory, DNA coding is used to mystifying and scatter the data (audio). | New audio encryption method offer very high standard terms in security | Encryption process used only for single and dual audio format |
| 3 | Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption | Biometric template existing safeguard schemes may downgrade granting capability or problem based on speed and security | Approach by fusion of fuzzy extractor with a novel bit-wise encryption scheme to engender cancelable biometric templates | The scheme that safeguard without supplementary noise that means of bit errors is executed in preserved template | Metamorphic fuzzy extractor takes enormous vast repository |
| 4 | PSDS– Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud | Data security problems over multi cloud such as vulnerable to numerous attacks. | Sensitive are divide into two parts, it encrypted separately and stored in different cloud storage | Proposed method is used to secure against following attack, related key attack, man- | The processing time and complexity for encryption authentication is very high |

| | | | | | |
|---|---|---|---|---|---|
| | | | | in middle attack, pollution attack | |
| 5 | Image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map | Single dimensional chaotic encryption algorithm has descent capability but huge problem is too small space for key | 2D chaotic system is fusion of sine maps along with logistic map. The sine map makes on combination of two chaotic maps combining encryption design for a multiple DNA encode and decode. | Algorithm achieved they are key sensitive, histogram and correlation analysis. It makes difficult for most successful attack | Algorithm has limitation is that only diffusion is used during the encryption process |
| 6 | Memorable Image Encryption Algorithm Based on Neuron-Like Scheme | Image cryptographic algorithm facing problems, makes lead to data insensitivity in system for equivalent keys | Neuron-like based learning scheme makes to identify a catchy scattered scheme and execute the plaintext based image encryption algorithm. The process get input and weights of the neuron through the feedback operation to regulate the information of image | It results high security and adaptive characteristics | Secret key used in the encryption process is 512-bit long |
| 7 | Enhanced secure data backup | Intruder can intrude any important | Encryption process done before the | Multifactor authentication is provided | Process of hiding the key is more complex |

| | | | | | |
|---|---|---|---|---|---|
| | scheme using multi-factor authentication | information on mode of transfer | transmit data for cloud storage. The design hidden sharing method and multi-factor authentication provide data protection | secure data with enhanced data backup process using own password and biometric | and backup process have to enhance |
| 8 | Image Encryption Algorithm Using a Novel Key-Substitution Architecture | Existing image encryption allows lack of safety and encryption capability has below the par | Encryption architecture (KSA) progressing key for upgrade the commencing keys implement plain image and evolve another substitution scheme that encrypting different category images | Proposed substitution method which establish on s-boxes to different categories image encryption | Algorithm have very complex throughput process |
| 9 | Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage | Random data blocks that verify data integrity inadequate involve highly sensitive data | CAPDP allows storage user to do data integrity verification infinite | The verification process is self-reliant of the count of blocks being checked | Data owner must store accumulator and tag record table. |
| 10 | Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete | Recent chaotic image encryption algorithm unable to block chosen plaintext attack | DNA encoding and decoding schemes invoke plain image correlated DNA order progress further dependent on hashed data | Makes unworkable for intruder to deploy of special plain-image attack | Algorithm have low encryption efficiency |

| | | | | | |
|---|---|---|---|---|---|
| | Logarithm | | | | |
| 11 | Fast Phrase Search for Encrypted Cloud Storage | Identifying with keywords search may causes bugs named fuzzy keywords | Phrase search based Bloom filters uses services of n-gram filters to adopt functionality and it allows phrase search to execute self-sustain without initial progression of conjunctive keyword based search that detect user files | Algorithm is modified to enhance topmost speed or topmost speed along a adoptable repository cost | Phrase search based encryption for cloud storage is not explored ate. |
| 12 | Traceable Anonymous Authentication and Key Exchange Protocol for Privacy-Aware Cloud Environments | Anonymous ID-theft attacks is block | Pre-authentication and post authentication of user to avoid anonymity. | Protection support quick bug identifying or offline security upgrade to trace illegal users. | User registration phase system authority has to identify suspected user. |
| 13 | High Throughput and Secure Authentication -Encryption AES-CCM Algorithm on Asynchronous Multi core Processor | Analysis of AES-CCM algorithm in asynchronous multi core processer | Matrix transformation based on authentication and parallel encrypting process established on multi-core processor | Helps active high through put, comprehension performance and secure AES based on counter with chaining mode | Processing speed of same algorithm is differs due to multi core |
| 14 | Authentication by Encrypted Negative | Authentication techniques are despite some | Plaintext password to hashing | Technique is secure from lookup table | Hashing technique is used but still |

| | | | | | |
|---|---|---|---|---|---|
| | Password | security flaws | password, hashing password to negative password and finally using symmetric-key algorithm for creation encrypted negative password | attack as dictionary attacks | have improve the password security |
| 15 | Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding | Image encryption progress with the simple structure | Image hashed data to frequentative progressing aspect of matrix to enhance parameterized value of chaotic maps, it increases the association of key along with original image. The generation of any-order by chen's chaotic structure is processed for any-order encryption process the DNA coding and decoding process | Achieve solution for problem of counter statistical attacks, noise attack and robustness of cropping, plaintext sensitivity and differential attacks | Algorithm is too much complicated even it ensure the security |
| 16 | Network Coding and DES Based Dynamic Encryption | Protection in multiple defense in cyber security | Three layered dynamic encryption process depend upon DES along | Low complexity and strengthen the | Proposed algorithm is rather not up to the mark on equivalent of |

| | | | | | |
|---|---|---|---|---|---|
| | Scheme for Moving Target Defense | | with network coding, encryption process depends on the partial key update work done | adaptability of different cyber conditions | triple DES |
| 17 | Practical Discrete Gaussian Samplers for Lattice-Based Cryptography | Asymmetric cryptographic are required large amount of computation and storage | The elliptic curve cryptography is used to decreases power consumption, increases devices performance. Secure and Efficient Encoding scheme to address the encoding part, eventually important to secure the mapping of the message and it benefits by resisting to several attacks | Have strong enforcement to conform secure communication especially when the message is encoding in elliptic curve | Algorithm is focus mostly in side channel time attacks |
| 18 | secure data backup scheme using multi-factor authentication | Intruder can intrude any important information on mode of transfer | User using a symmetrical key and divided it into three shares, save the shares and delete the key. To access the data, key can reconstruct easily by combining the shares in user’s | Smart devices lost and damage they use, the password and biometric for recovery process | Purpose of deleting the key is duplicate by weak security backup |

| | | | | | |
|---|---|---|---|---|---|
| | | | smart devices. | | |
| 19 | Efficient Public Verification of Data Integrity for Cloud Storage Systems from In distinguishability Obfuscation | The outsourcing the date is the problem for Data integrity | Audition at most required to evaluate message validity code tag for validation. It is self-sustained with number of validation works | Achieves light weight verification in auditor side | Auditor is playing major role in this algorithm. There are more possibilities due to human errors |
| 20 | AES-Like Cipher and Its White-Box Implementation | Providing more protection in round execution process in AES | AES-Like Cipher, protecting encryption key during the execution of the AES algorithm in open sources devices. It is depend on key-driven S-boxes key expansion. The S-boxes works as a key expansion and these S-boxes is applied to all the round keys. | The S-boxes is used to preventing the known white-box attacks | S-boxes is very efficient in protection of data but still execution is long |
| 21 | Two-Factor Data Security Protection Mechanism for Cloud Storage System | Increasing authentication to protect our data in cloud storage | Two-factor authentication for data security prospection process with element mutable in cloud storage environment | Encrypted data transfer through the cloud from sender to receiver but decryption process is done by two keys, first is | Two-factor authentication is not enough to secure data in current environment |

| | | | | | |
|---|---|---|---|---|---|
| | | | | secret key and another one is unique key. | |
| 22 | Robust Stability Assessment in the Presence of Load Dynamics Uncertainty | Dynamic response of loads inherent uncertainty and natural variability makes difficult and compromise the security | Judgment of a little- signed constancy of operating points with new proposed novel mathematical “robust stability” criterion. It helps to provides mathematical promise stability of the operation point for any multiple connection of loads | RSA prosper to confirm the solidity the ability without making any speculation on the multiple response for load | Theft constancy regime can be executed in designing and operations absence of differentiate efficiency and economic factors |
| 23 | On the Security of 2-Key Triple DES | Reconsiders the safety offered by two key triple DES | Suggest 80 bits of security key is better than 56 bits of securities. | van oorstch-wiener attack which is executed with both cipher text and plaintext sets produce utilizing a variety keys | The key change in regular interval helps to minimum the impact of successful attacks but it does not minimal the attack’s success probability |
| 24 | Distance-Based Encryption Fuzziness in Biometric-Based Encryption | Encryption algorithm is executed by value of biometric as encryption key | Encryption phase biometric scanned a private key to get encrypted cipher ,in key generation phase with another | Both encrypted chipper and decrypt chipper key get after the biometric authenticatio | Providing same biometric authentication for both chipper test and key make monopoly |

| | | | | | |
|---|---|---|---|---|---|
| | | | biometric scanned a private key can decrypt a cipher key | n process and executes normal encryption | |
| 25 | Security of an Efficient Dynamic Auditing Protocol in Cloud Storage | The outsourcing the date is the problem for Data integrity | Proposed most effective multiple verifying protocol transaction depend upon distributed along with parallel system | Auditor can detected arbitrarily modified cloud data in auditing process | Auditor is playing major role in this algorithm. There are more possibilities due to human errors |
| 26 | Role-Based Access Control on Encrypted Data in cloud storage | Control and prevent of unauthorized access in cloud storage | Incorporate the cryptographic techniques with pole based access control is named as role based encryption | safe RBE-based combination of cloud storage environment permit a concern to save records assumed on public storage and storing confidential data in private cloud storage | No separate encryption algorithm of sensitive data |

## 4. CONCLUSION

The analysis of the following literatures and comparisons of methodology, problem definition, implication, merits and demerits. Thus, the motivation of cryptographic encryption and decryption process is common for image, audio, video and text to secure these types of data. But the existing methodology differs depend upon the types of data. According to the observation conclude to propose new encryption and decryption algorithm scheme that generalized for all types of data with high efficient and secure technique without storing secret keys in database. To design and develop new algorithm scheme to get the credentials that based on the user unique and credentials not stored and maintained in cloud storage.

## REFERENCES

[1]. S. Atiewi et al., "Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptography," in IEEE Access, vol. 8, pp. 113498-113511, 2020, doi: 10.1109/ACCESS.2020.3002815.

[2]. X. Wang and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," in *IEEE Access*, vol. 8, pp. 9260-9270, 2020, doi: 10.1109/ACCESS.2019.2963329.

[3]. D. Chang, S. Garg, M. Hasan and S. Mishra, "Cancelable Multi-Biometric Approach Using Fuzzy Extractor and Novel Bit-Wise Encryption," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3152-3167, 2020, doi: 10.1109/TIFS.2020.2983250.

[4]. F. Shahid, H. Ashraf, A. Ghani, S. A. K. Ghayyur, S. Shamshirband and E. Salwana, "PSDS–Proficient Security Over Distributed Storage: A Method for Data Transmission in Cloud," in IEEE Access, vol. 8, pp. 118285-118298, 2020, doi: 10.1109/ACCESS.2020.3004433.

[5]. J. Zheng and L. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map," in *IET Image Processing*, vol. 14, no. 11, pp. 2310-2320, 18 9 2020, doi: 10.1049/iet-ipr.2019.1340.

[6]. Y. Zhang and B. Li, "The Memorable Image Encryption Algorithm Based on Neuron-Like Scheme," in *IEEE Access*, vol. 8, pp. 114807-114821, 2020, doi: 10.1109/ACCESS.2020.3004379.

[7]. H. Hu, C. Lin, C. Chang and L. Chen, "Enhanced secure data backup scheme using multi-factor authentication," in IET Information Security, vol. 13, no. 6, pp. 649-658, 11 2019, doi: 10.1049/iet-ifs.2018.5380.

[8]. Y. Song, Z. Zhu, W. Zhang, H. Yu and Y. Zhao, "Efficient and Secure Image Encryption Algorithm Using a Novel Key-Substitution Architecture," in *IEEE Access*, vol. 7, pp. 84386-84400, 2019, doi: 10.1109/ACCESS.2019.2923018.

[9]. W. I. Khedr, H. M. Khater and E. R. Mohamed, "Cryptographic Accumulator-Based Scheme for Critical Data Integrity Verification in Cloud Storage," in IEEE Access, vol. 7, pp. 65635-65651, 2019, doi: 10.1109/ACCESS.2019.2917628.

[10]. W. Feng, Y. He, H. Li and C. Li, "A Plain-Image-Related Chaotic Image Encryption Algorithm Based on DNA Sequence Operation and Discrete Logarithm," in *IEEE Access*, vol. 7, pp. 181589-181609, 2019, doi: 10.1109/ACCESS.2019.2959137.

[11]. H. T. Poon and A. Miri, "Fast Phrase Search for Encrypted Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 7, no. 4, pp. 1002-1012, 1 Oct.-Dec. 2019, doi: 10.1109/TCC.2017.2709316.

[12]. H. Lin, "Traceable Anonymous Authentication and Key Exchange Protocol for Privacy-Aware Cloud Environments," in IEEE Systems Journal, vol. 13, no. 2, pp. 1608-1617, June 2019, doi: 10.1109/JSYST.2018.2828022.

[13]. A.A. Pammu, W. Ho, N. K. Z. Lwin, K. Chong and B. Gwee, "A High Throughput and Secure Authentication-Encryption AES-CCM Algorithm on Asynchronous Multicore Processor," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1023-1036, April 2019, doi: 10.1109/TIFS.2018.2869344.

[14]. W. Luo, Y. Hu, H. Jiang and J. Wang, "Authentication by Encrypted Negative Password," in IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 114-128, Jan. 2019, doi: 10.1109/TIFS.2018.2844854.

[15]. Q. Zhang, J. Han and Y. Ye, "Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding," in *IET Image Processing*, vol. 13, no. 14, pp. 2905-2915, 12 12 2019, doi: 10.1049/iet-ipr.2019.0667.

[16]. H. Tang, Q. T. Sun, X. Yang and K. Long, "A Network Coding and DES Based Dynamic Encryption Scheme for Moving Target Defense," in IEEE Access, vol. 6, pp. 26059-26068, 2018, doi: 10.1109/ACCESS.2018.2832854.

[17]. J. Howe, A. Khalid, C. Rafferty, F. Regazzoni and M. O’Neill, "On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography," in *IEEE Transactions on Computers*, vol. 67, no. 3, pp. 322-334, 1 March 2018, doi: 10.1109/TC.2016.2642962.

[18]. Y. Liu, Q. Zhong, L. Chang, Z. Xia, D. He and C. Cheng, "A secure data backup scheme using multi-factor authentication," in IET Information Security, vol. 11, no. 5, pp. 250-255, 9 2017, doi: 10.1049/iet-ifs.2016.0103.

[19]. Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu and X. Zhang, "Efficient Public Verification of Data Integrity for Cloud Storage Systems from Indistinguishability Obfuscation," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 676-688, March 2017, doi: 10.1109/TIFS.2016.2631951.

[20]. K. Bai and C. Wu, "An AES-Like Cipher and Its White-Box Implementation," in The Computer Journal, vol. 59, no. 7, pp. 1054-1065, July 2016, doi: 10.1093/comjnl/bxv119.

[21]. J. K. Liu, K. Liang, W. Susilo, J. Liu and Y. Xiang, "Two-Factor Data Security Protection Mechanism for Cloud Storage System," in IEEE Transactions on Computers, vol. 65, no. 6, pp. 1992-2004, 1 June 2016, doi: 10.1109/TC.2015.2462840.

[22]. H. D. Nguyen and K. Turitsyn, "Robust Stability Assessment in the Presence of Load Dynamics Uncertainty," in *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1579-1594, March 2016, doi: 10.1109/TPWRS.2015.2423293.

[23]. D.Godwin Immanuel, Dayana D.S, Sindarsingh Jebaseelan S.D “Hybrid Genetic Algorithm Assisted Artificial Bee Colony Approach for Voltage Stability Improvement” International

Journal of Applied Engineering Research ISSN No.0973-4562 Research India Publications, Volume 10, Number 59 (2015) pp.534-541.

[24]. C. J. Mitchell, "On the Security of 2-Key Triple DES," in *IEEE Transactions on Information Theory*, vol. 62, no. 11, pp. 6260-6267, Nov. 2016, doi: 10.1109/TIT.2016.2611003.

[25]. F. Guo, W. Susilo and Y. Mu, "Distance-Based Encryption: How to Embed Fuzziness in Biometric-Based Encryption," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 247-257, Feb. 2016, doi: 10.1109/TIFS.2015.2489179.

[26]. D. Godwin Immanuel and C. Chritober Asir Rajan, "An Genetic Algorithm approach for reactive power control problem," 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, 2013, pp. 74-78, doi: 10.1109/ICCPCT.2013.6528940.

[27]. J. Hong, K. Xue and W. Li, "Comments on “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems”/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1315-1317, June 2015, doi: 10.1109/TIFS.2015.2407327.

[28]. P. Roberto de Oliveira, V. Delisandra Feltrim, L. Andreia Fondazzi Martimiano and G. Brasilino Marcal Zanoni, "Energy Consumption Analysis of the Cryptographic Key Generation Process of RSA and ECC Algorithms in Embedded Systems," in *IEEE Latin America Transactions*, vol. 12, no. 6, pp. 1141-1148, Sept. 2014, doi: 10.1109/TLA.2014.6894012.

[29]. Godwin Immanuel, D., Dayana, D.S, Solar water pumping system using enhanced DC–DC converter, Journal of Advanced Research in Dynamical and Control Systems, vol.10,2018,1609-1614.

[30]. J. Ni, Y. Yu, Y. Mu and Q. Xia, "On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 10, pp. 2760-2761, Oct. 2014, doi: 10.1109/TPDS.2013.199.

[31]. L. Zhou, V. Varadharajan and M. Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," in IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, Dec. 2013, doi: 10.1109/TIFS.2013.2286456.

[32]. Cryptography and Network Security 3rd Edition, authored by Atul Kahate, is a comprehensive book.