MJSAT

Malaysian Journal of Science and Advanced Technology

journal homepage: https://mjsat.com.my/

Constructing a Secure Data Storage System That Supports Multiple Functions by Using Key Aggregation for Data Sharing in Cloud Storage: A Review

Othman Atta Ismael*[1]

[1] *Dept. of Networks, Al Iraqia University/ College of Engineering. Baghdad, Iraq.*

KEYWORDS

Data encryption
Data security
Key aggregation
Cloud Storage
Cloud security

ARTICLE HISTORY

Received 30 January 2022
Received in revised form 16 February 2022
Accepted 17 February 2022
Available online 18 February 2022

ABSTRACT

The old method used for examining data correctness is to recover the entire data from the cloud and then validate data reliability by scrutinizing the correctness of signatures or numeric values of the data as a whole. In modern cryptology, an essential problem to study here is to maintain the greatest benefit of the privacy of given information to perform multiple encryptions. The study shows how a decryption key is made stronger in the sense that it enables several ciphertexts to be decrypted without increasing their size. The statement of the problem lies in the fact that creating an effective public-key encryption system that supports flexible delegation is decipherable by a fixed-size decryption key that could be produced by the holder of the master-secret key. The solution to this problem is by presenting a definite type of public-key encryption known as key-aggregate cryptosystem (KAC). By using this method, users who hold master-secret key could convert a message through a public-key, and an identifier of ciphertext called "class". This means that the ciphertexts could be further categorized into various classes. The main objective of this paper is to design a secure data storage system that provides multiple stimulating functions by which the storage system is divided and has no major authority.

1. INTRODUCTION

The study suggests a safe cloud storage system that efficiently supports protecting public auditing mechanism in cloud computing. We use the homomorphic linear authenticator (HLA) and random masking technique to guarantee that the third -party auditor (TPA) would not identify about the stored data on the cloud server while during the operational auditing process, which does not only eliminate the negative impact of cloud user from the dull, but also ease the users' fear of their outsourced data leak [1].

By restoring to the storage of online data in a cloud environment, users can easily and remotely store their data and enjoy premium and handy services and applications from a shared pool of configurable computing resources, without bearing the negative impact of maintenance and local data storage. However, what makes the task of data reliability protection in cloud computing difficult is the lack of physical possession of the outsourced data, especially for users who have limited computing resources. Besides, users must use the local storage of online data in a cloud environment without worrying about the authentication of its integrity. Thus, it is so important to enable public auditability for the storage of online data in a cloud environment so that users can turn to a third-party auditor (TPA) to check the authenticity of the data management paradigm easily. To introduce an effective and secured TPA, the auditing process should prevent new exposures to user's data privacy and abandon additional online burden. Therefore, we suggest a secure storage of online data in a cloud environment system that maintains privacy-preserving public auditing.

Then we work on enhancing the TPA to perform audits instantaneously and competently for multiple users. Comprehensive security and performance analysis show that the proposed systems are proved to be secured and highly effective. The preliminary experiment that has been applied on Amazon EC2 shows the performance of the design was adequate [2].

*Corresponding author:
E-mail address: Othman Atta Ismael < othman.atta@yahoo.com >.

2. DEFINITION OF BASIC TERMS

The most important brief definitions of the basic terms mentioned in the title of the research are as follows:

2.1 Data Storage Systems

whilst data storage has a history closely related to its computing, research data offers a mite of novel and unique obstacles, particularly when it comes to confidentiality and persistence. commonly most technical details will be dealt with it by expert professionals, but collecting the main understanding of the internal workings, Benefits, and limitations of the different options can help put data management plans customized to the requirements of each study project, subject area, or community [3].

2.2 Data sharing

Data sharing is the quest for making data and information utilized for all and accessible to different people [4].

2.3 Semantic technology

The word "semantic" refers to meaning in language.

Semantic technology utilizes formal semantics to assist artificial intelligence (AI) systems realize language and process data and information the manner in which people do. Accordingly, they can store, oversee, and recover information dependent on logical relationships and meaning. Different organizations and businesses are now utilizing semantic graph databases semantic technology to manage their content, repurpose and reuse information, cut expenses, and gain new income streams.

Semantic technology is a bunch of methods and strategies and tools that give advanced means for processing and categorizing data [5].

3. EXISTING SYSTEM

Several tools have been utilized to allow a data owner and also a third-party auditor to competently execute integrity examination without transferring the whole data from the cloud. The process is called public auditing. According to these tools, data is split into many small blocks, where each block is individually signed by the owner. Thus, an arbitrary grouping of all the blocks is recovered during integrity examination. A third-party auditor could be a data user (for example researcher) who might be involved in using the owner's data by the cloud or a third-party auditor (TPA) who can provide expert integrity monitoring services [6] An advanced auditing framework was developed by Wang et al. So, that during public auditing on cloud data. Regrettably, current public auditing solutions deal with personal data in the cloud only. They think that making data between multiple user's public might be one of the most appealing characteristics and features that motivate the storage of online data in a cloud environment.

Accordingly, they should guarantee that the integrity of shared data is correct in the cloud. Present public auditing mechanisms can essentially be expanded to validate the integrity of shared data. However, they should notice that one of the substantial privacy problems concerning shared data is the use of existing tools that results in leaking identity privacy to public verifiers. Considering data confidentiality, a traditional way to ensure the server that administers the access control after data being authenticated means that any unforeseen vulnerability will endanger all data. Things get complicated in a shared cloud computing environment.

In the case of the accessibility of files, there is a sequence of cryptographic procedures that allow a third-party auditor to check the accessibility of files on behalf of the data owner without risking anything about data, or without revealing the data of the owner's anonymity. On the other hand, cloud users do not strongly rely on a cloud server in accomplishing tasks that suit confidentiality [7] [8].

Securing a cryptographic solution that depends on number theoretic presumption is more helpful, whenever it perfectly satisfies the user with the security of the VM or the reliability of the technical staff [9].

4. PROPOSED SYSTEM

In this study, we use a private key to decipher multiple ciphertexts to allow decrypting multiple ciphertexts, without increasing its size and each ciphertext is encrypted with a different public or identity key. Since the statement of the problem is to present competent public-key cryptography, we recommend introducing a different type of cryptography, known as key-aggregate cryptosystem (KAC). In the case of KAC, users could encode a message either through a public key or through an identifier of ciphertext called class. A master-secret key is held by the key owner, that can be utilized to get secret keys for various classes. More significantly, the extracted key can also be a cumulative key that is compact as a secret key for a unified class, but combine the power of several like keys, in other words., the power that transforms encrypted data into its original form for any subdivision of ciphertext classes.

To maintain the privacy of shared data, we recommend using a novel privacy-preserving public examination technique for insurance shared data in the cloud called Oruta. To be more precise, we use the electronic signature technique to construct a multi-key homomorphic authenticators' scheme in Oruta, to facilitate a public verifier authenticating the reliability from shared data without improving the whole data. In this case, the identification from the subscriber on every block of the shared data should remain private so as not to be accessed by a public verifier. Furthermore, they expand our technique to archive batch proofing, that can carry out multiple auditing tasks equivalently and improve the efficiency of verification for multiple audit assignments. In the meantime, Oruta, which stands for "One Ring to Rule Them All" is consistent with random masking.

Wang et al. developed an innovative auditing procedure (called WWRL), so that through public audit on cloud information, the content of information owned by an individual customer is not made available to any public verifiers. Moreover, index look-up tables could be preserved from previous public auditing to support dynamic data. A multi-layered comparison between Oruta and the current mechanisms is identified.

5. SYSTEM ARCHITECTURE

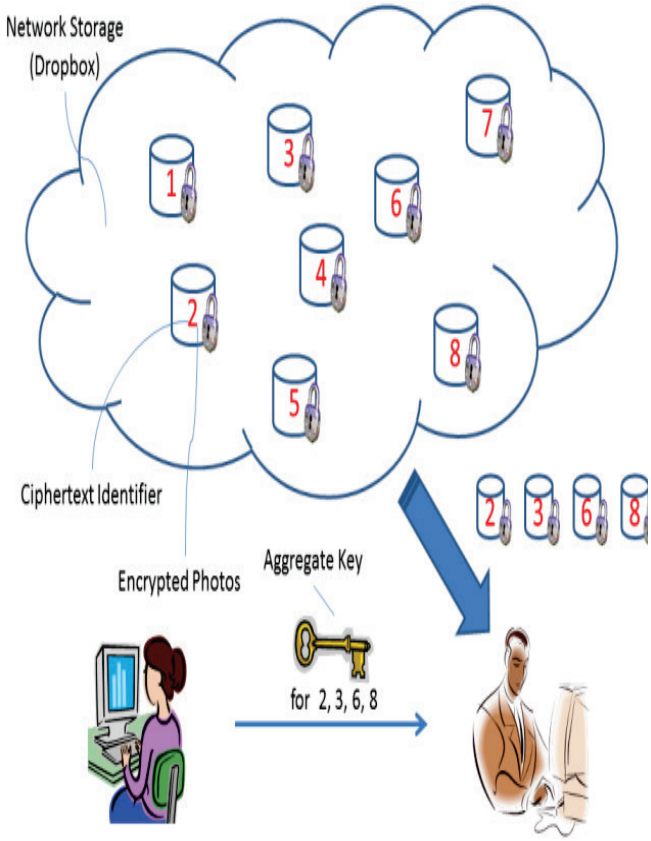

Fig. 1. System architecture [10].

6. MODULES AND ALGORITHMS

6.1 Key-aggregate cryptosystem (KAC)

They use a private key to decipher multiple ciphertexts to allow decrypting multiple ciphertexts, without increasing its size and each ciphertext is encrypted with a different public or identity key. Since the statement of the problem is to present competent public-key cryptography, they recommend introducing a different type of cryptography, known as key-aggregate cryptosystem (KAC). In the case of KAC, users could encode a message either through a public key or through an identifier of ciphertext called class. A master-secret key is held by the key owner, that can be utilized to get secret keys for various classes. More significantly, the extracted key can also be a cumulative key that is compact as a secret key for a unified class but combine the power of several like keys, in other words., the power that transforms encrypted data into its original form for any subdivision of ciphertext classes.

- **Framework**

The key aggregate encryption scheme comprises of five polynomial-time algorithms. They are per the following:

Step1. create and Setup the account on the server for sharing of data. This account is created by a data proprietor.

Step2. The keyGen algorithm is utilized for the generation of a public key. The data proprietor produces a public secrete key to encrypt the data across the cloud. It also creates an aggregate key to arrival the block of ciphers of fixed size.

Step3. Encodes the information and data given by the data proprietor by utilizing the secrete key. This encrypted information and data are then shared between the cloud.

Step4. The aggregate key is utilized for extracting the specific block of the ciphers from the cipher file. Yet, other encrypted information and data stay secure.

Step5. Decrypt or can say decode: The encoded information and data is then decoded by utilizing the same secrete key whose is utilized for encryption [11].

6.2 User registration and control

By using this module, the admin will be responsible for the user's registration process. Here, users give their individual details for registration operation. Each user will have an ID to log into the cloud space after registration. If the users want their information to be modified, they must send the details to the admin. Afterward, the admin will perform the process of editing and updating the information. Thus, the whole process is regulated by Admin [12].

6.3 Sharing information's

In this module, Users share their data and information using the aggregate key in their own admin-provided cloud space. This information might include significant data. To guarantee the security of their information, users store the information in their particular cloud. Data can only be saved in the cloud by registered users [13].

6.4 Encryption process

In this module, Triple DES (Data Encryption Standard) algorithm is used to encode the information and data shared in the cloud. So, all of the information shared by every user is encoded and stored in the cloud [14].

6.5 Checking integrity

The integrity-examination mechanism is an operation to verify if the information has not changed and to match encoded information with modified text cryptographic. If there is some modification in discovery, a message will be sent to the user which the encryption operation isn't being implemented correctly. If no shift in detection exists, it means that the next operation is allowed to be performed. Checking integrity is primarily used to monitor anti-malware [15].

6.6 Data confidentiality

The cloud clients need to ensure that their information substances are not made accessible or unveiled to unlawful clients. Just approved clients can get to the touchy information while others ought not to get to any data of the information in the cloud.

6.7 Fine-grained access control

Information proprietors can confine the unapproved clients to get the information moved to the cloud. The information proprietor awards different access privileges to a bunch of clients to get to the information, while others are not permitted to access it without consent. The entrance consent ought to be controlled simply by the proprietor in un-confided cloud conditions.

6.8 Callable and Efficient

The quantity of Cloud clients is incredibly huge and the clients join and leave unusually, it is fundamental that the framework keeps up with effectiveness as well as versatility. Powerful information partaking in distributed computing framework should fulfill all the security prerequisites [16].

6.9 Data forwarding

According to this module, by using the public key of that user, they could be sent encoded data or information stocked in the cloud to another user account. If any user needs to share their information with anyone, the encoded information can be forwarded to them immediately. Thus, the user can forward the information to another user without the need to download the data.

6.10 Data extraction

The decryption process is used to convert plaintext into ciphertext. The encoded data is deciphered by the user using the owner's public key. To encrypt and decrypt the information, the Triple-DES algorithm is utilized, so that the user can access, view, download, and protect the digital data.

6.11 DES (Data Encryption Standard)

DES operates on bit strings, or binary numbers, popular to digital computers—the 0s and 1s. Every four-bit group consists of hexadecimal, or base16, number. Thus, binary "0001" is congruent to the hexadecimal number "1", binary "1000" is equal to the hexadecimal number "8", and binary "1001" is congruent to the hexadecimal number "9". On the other hand, the hexadecimal number "A" is equal to binary "1010" and the hexadecimal number "F" is congruent to binary "1111".

DES's work is based on encoding batches of 64 message bits, that is equal to 16 hexadecimal numbers. DES uses "keys" to be doing the coding, seemingly including 16 hexadecimal numbers long or 64 bits long. In the DES algorithm, however, every 8th key bit is ignored, so that the actual key size reaches 56 bits. But, in every situation, DES is formed by the combination of 64 bits (16 hexadecimal digits).

For instance, if they encode the plaintext message "8787878787878787" with the DES key "0E329232EA6D0D73", they come up with the ciphertext "0000000000000000". But if the ciphertext is converted with the same secret DES key "0E329232EA6D0D73", they get the original plaintext "8787878787878787". This example is well-ordered and logical because our plaintext was precisely 64 bits long and the same would be true if the plaintext comes about a multiple of 64 bits. But most messages will not come under this category. They will not be exactly as multiple of 64 bits (that is to say, an exact multiple of 16 hexadecimal numbers).

The running example: "Your lips are smoother than Vaseline" which has been taken from J. Orlin Grabbe, The DES Algorithm Illustrated, http://orlingrabbe.com/des.htm, is 38 bytes (76 hexadecimal digits) long. So, this message must be supported with some extra bytes by the end of the encoding. Once the encrypted message has been decrypted, these extra bytes are discarded. There are, obviously, different padding systems--different ways to add extra bytes. To come up with the total message of a multiple of 8 bytes (or 16 hexadecimal digits, or 64 bits), they need to add 0s at the end. This means that the plaintext message "Your lips are smoother than vaseline" is, in hexadecimal, "596F7572206C6970 732061726520736D 6F6F746865722074 68616E2076617365 6C696E650D0A".

They should notice here that the first 72 hexadecimal digits signify the English message, while "0D" is hexadecimal for Carriage Return, and "0A" is hexadecimal for Line Feed. This shows that the message file has ended. After that, they detect this message at the end with some 0s to get a total of 80 hexadecimal digits: "596F7572206C6970 732061726520736D 6F6F746865722074 68616E2076617365 6C696E650D0A00 00".

But they get the ciphertext: "C0999FDDE378D7ED 727DA00BCA5A84EE 47F269A4D6438190 9DD52F78F535 8499 828AC9B453E0E653" in case they encode the plaintext message 64 bits (16 hexadecimal digits) by using the same DES key "0E329232EA6D0D73" as before.

This is the secret code that can be conveyed or stored. Decrypting the ciphertext brings back the original message "Your lips are smoother than Vaseline"[17] [18].

6.12AES (Advance Encryption Standard)

(AES) in cryptography is a class of symmetrical-key encryption algorithms which has been developed to be used in cloud data security. A 128-bit block size supports every one of the ciphers, with key sizes of128, 192, and 256 bits, respectively. AES functions on a 4 * 4 column - main order matrix of bytes. AES algorithm came up as a complementary algorithm to the DES as its working mechanism was similar but the prior one performed better on the security standards compared to the latter one. AES is an algorithm that can be implemented at both hardware as well as software levels. This algorithm provides a lot of scope for developers as well as researchers to make the mathematical changes in the algorithm to make it deployable for the service requirement [19] [20] [21].

- **EXAMPLES**

Twenty examples are given to explain the MAC process of generating. The fundamental block cipher is either the TDEA or AES algorithm. The block cipher key is installed for each of the present passable key sizes, in other words, AES-128, AES-192, AES-256, two key TDEA, and three key TDEA. For any key, the corresponding subkey generation is given, accompanied by four examples of MAC generation using the key. The messages in any example set are acquired via shortening a 64-byte common fixed string. Whole strings are exemplified in hexadecimal code, with a space (or a new line) introduced in all 8 symbols, for reading. K1 and K2 are recommended to represent the sub keys, M to represent the message, and T to represent the MAC. For the AES algorithm examples, Tlen is 128, i.e., (32) hexadecimal symbols, and (K) represents the key. For the TDEA examples, Tlen is 64, in other words, 16 hexadecimal symbols, and the key, (K), is the ordered triple of strings, (Key1, Key2, and Key3). For two key TDEA, Key1 = Key3. D.1 AES-128 [20].

7. PRIVACY-ASSURED AND EFFECTIVE CLOUD DATA UTILIZATION

To protect data privacy and stop unwanted accesses in the cloud and beyond, sensitive data has to be encrypted before outsourcing which produces operational data service this is

based on a searchable keyword in plain text. So, permitting an encoded cloud data search service alongside assuring privacy is of great significance. This issue is mostly challenging considering the likely great number of on-demand data users and great numbers of outsourced data files in the cloud, as it is really difficult to meet the performance, system usability, and scalability requirements as well. The study seeks to utilize privacy-assured cloud data with functioning, high performance, and usable service. This is done by implementing two daunting tasks: unsure keyword exploration and ranked keyword exploration through encrypted cloud data.

Unsure keyword exploration, disagree to exact keyword matching, accepts only minor spelling mistakes or minor typographical errors and format irregularities in user search demands, and significantly improves the usability of the system and the user experience in searching. The problem stems from the truth that two words similar to one other would not be the same after a one-way compression function for the searching encoded keyword. To solve the issue, they design brand new symbol-based tries adapted in index construction to provide search efficiency. Classified keyword search also secures the accuracy of file recovery and helps the user to effectively locate the most/least important information [22].

8. SCALABLE AND OWNER-CONTROLLED CLOUD COMPUTING DATA SHARING

Different sensitive data accumulated in cloud computing requests the cloud data sharing service to be accountable for safe, effective, authoritative, and secure access to data content between several users on behalf of data owners. As cloud computing server may be no longer be in the selfsame reliable domain like the Data holders, in this open world and environment, they have to rethink the issue of access control. Here, the cloud computing server takes whole control over the administration of the pre-processed data owner which isn't necessarily trusted regarding data privacy. Three factors make the problem more demanding which are: the imposition of Very accurate data access, the support of access privilege updates in dynamic scenarios, and the system flexibility while preserving low-level complications of key administration and data encoded. The aim is to provide tools that make cloud data access completely managed by the owners and enable all owners/users to profit very well from current secure cloud data sharing services skills.

To keep fine-grainedness, they recommend treating data to be viewed like files linked to a group of significant attributes, using the logical composition of attributes to demonstrate fine-grained access to data, and enable an owner to take control across attribute-based cryptography. For built-in scalability requirement for a cloud computing system, where user access privilege updates occur often and so inevitably sustains significant user/ data administration load on data owner.

Furthermore, cloud computing should be treated as a mediated agent so data owners can tackle a more difficult workload, as handling user access privilege dynamics in a big system, without prejudice the basic data privacy. Furthermore, they explore other security targets in a practical cloud computing data sharing system, Including confidentiality of user access privilege and user liability in the event of abuse of user access key attacks. They think those efforts will result in an integrated end solution for the implementation of a more realistic data sharing service in the cloud [23].

9. SECURE DATA COMPUTATION OUTSOURCING IN CLOUD

The main concern of transferring computing workloads for special resources into cloud computing is the security of private data consumed and produced by computing. so, secure computation outsourcing services are in dire need to not only protect sensitive workload information and also to authenticate the safety of the computation outcome. However, this is a very challenging job due to many problems that need to be tackled immediately. First, as a service must be practically feasible with regard to computational complexity [24]. Second, it must have a sound security warranty without restrictive laws for the system. Thirdly, it should let considerable computational efficiencies be used by end-user, compared to efforts exerted to solve the problem locally. The challenges rule out presenting the existing techniques that have been developed to improve fully secured multi-party computation and homomorphic encryption.

Keeping the above challenges in mind, the research studies secure cloud-based outsourcing services. They concentrate on vastly relevant engineering computing and optimization problems. Our approach is to plainly break up computations into general programs and special data and leverage the structures of particular computations of reaching desired alternations between safety, competence, practicality, and security. They seek to form those secure cloud-based outsourcing techniques in a hierarchy order, where computation can be calculated at different levels of abstraction, as the above-mentioned trade-offs can also be flexibly examined in a systematic way.

The study investigates two essential mechanisms that provide security services that include namely outsourcing systems from linear equations (LE) and namely secure outsourcing linear programming (LP) in cloud computing. Those two mechanisms are one of the most commonly utilized algorithmic and mathematical methods in different engineering fields the scrutinize and improve everyday-life systems. The study will be helpful for further research projects dealing with computational issues, like secure outsourcing of convex programming in cloud computing [25] [26].

10. SECURITY AND PRIVACY ISSUES IN DATA STORAGE

Cloud Computing permits the clients to store their data on the storage location kept up with by a third party. When the data is uploaded and transferred into the cloud the client loses its command over the information and data and the information and data can be altered by the assailants and the attackers. The assailants and the attacker may be internal(CSP) or external. Unauthorized and unapproved access is additionally a typical practice because of feeble access control. The security of data emerges the accompanying difficulties: The security and protection issues identified with information and data storage stockpiling are confidentiality, integrity, and availability [27].

11. CONCLUSIONS

Cloud Computing is becoming increasingly popular and progressing day by day. But still, the security threat hinders

the success of cloud computing and data privacy is essential in the cloud to ensure that the user's identity is not leaked to unauthorized persons. Using the cloud, anyone can share and store the data, as much as they want. To share the data in a secure way, cryptography is very useful. By using different encryption techniques. The researcher in this paper, have come up with the following results:

1. The use of existing tools in the existing System maybe results in leaking identity privacy and data to public verifiers.
2. In this paper, some of the privacy threats are addressed and the techniques to overcome them are surveyed.
3. Comprehensive security and performance analysis show that the proposed systems are proved to be secured and highly effective.
4. In the proposed system a safe cloud storage system that efficiently supports protecting public auditing mechanism in cloud computing.
5. In the proposed system technique guarantee that the third-party auditor (TPA) would not identify the stored data on the cloud server while during the operational auditing process, which does not only eliminate the negative impact of cloud user from the dull but also ease the users' fear of their outsourced data leak.
6. In the proposed system, that maintains privacy-preserving public auditing.
7. In Proposed system technique is to maintain the greatest benefit of the privacy of given information to perform multiple encryptions.
8. In the proposed System Checking integrity is primarily used to verify if the information has not changed and monitor anti-malware.
9. Cloud users assured that their data is stored, processed, accessed, and audited in a secured manner at any time, by using DES and AES in the proposed system.

REFERENCES

[1] K. M. Patel, and S. S. Bahekar, "Study on Homomorphic Linear Authenticator in Wireless Ad Hoc Networks ", IJIREEICE, Vol. 5, 2017, pp. 16-19.

[2] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on Computers, vol. 62, no. 2,2013, pp. 362-375.

[3] C. F. Blumzon, and A.-T. Pănescu, Data Storage, Cham: Handbook of Experimental Pharmacology, vol 257. Springer, 2019.

[4] "Data sharing," Wikipedia, the free encyclopedia. April. 31, 2016. [Online]. Available: https://en.wikipedia.org/wiki/ Data_sharing. [Accessed Apr. 15, 2021].

[5] J. Melesko, and E. Kurilovas, " Semantic Technologies in e-Learning: Learning Analytics and Artificial Neural Networks in Personalised Learning Systems", in Proceedings of the 8th International Conference on Web Intelligence, Mining and Semantics, 2018, Vol. 34, pp. 1-7.

[6] M. M. Ruke, S. Gore, S. Chavan, and prof : B. Dakhare, " Maintaining Data Integrity For Shared Data In Cloud", Advanced Computing: An International Journal, Vol. 8, No. ½, 2021, pp. 1 -8.

[7] B. Mahalakshmi, and G. Suseendran, " An Analysis of Cloud Computing Issues on Data Integrity, Privacy and Its Current Solutions ", Advances in Intelligent Systems and Computing, Vol. 2, 2020, pp. 467 -482.

[8] J. Li, H. Yan, and Y. Zhang, " Certificateless Public Integrity Checking of Group Shared Data on Cloud Storage ", IEEE Transactions on Services Computing, Vol. 14, No. 1, 2021, pp. 71 -81.

[9] B. Venkateswarlu, and G. V. Soumya, " Large Scale Data Storage and Retrieval System using Keywords for E-governance", International Journal on Future Revolution in Computer Science & Communication Engineering, Vol. 3, No. 10, 2017, pp. 163 -168.

[10] C. Chu, S. S. M. Chow, W. Tzeng, J. Zhou and R. H. Deng, " Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage ", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, 2014, pp. 468 -477.

[11] R. Veeravelli, " Data Sharing and Access Using Aggregate Key Concept", (M.S.) thesis, Department of Information Systems, St. Cloud State University, St. Cloud, United State, 2018

[12] S. Somasundaram, "Online Data Sharing Using Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 7, No. 4, 2019, pp. 2272 -2280.

[13] R. Veeravelli, " Data Sharing and Access Using Aggregate Key Concept", (M.S.) thesis, Department of Information Systems, St. Cloud State University, St. Cloud, United State, 2018.

[14] O.N. Akande, O.C. Abikoye, A.A Kayode., O.T.Aro, and O.R Ogundokun, A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security, Cham: Computational Science and Its Applications – ICCSA 2020 Springer, 2020.

[15] A. H. Kami, and Q. A. Hamad, " Achieve Data Security in Cloud Computing ", International Journal of Advances in Computer Science and Technology, Vol. 6, No. 11, 2017, pp. 25 -29.

[16] B.V.Varshini, M.Vigilson Prem and J.Geethapriya, "A Review on Secure Data Sharing in Cloud Computing Environment" , International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol 6, no 3, 2017, pp. 224- 228.

[17] Indumathi Saikumar. DES- Data Encryption Standard. IRJET [Internet]. 2017 Mar [cited 2021 Apr 21]; 4(3): 1777-1782. Available from: https://www.irjet.net/archives/V4/i3/IRJET-V4I3489.pdf

[18] I. Sumartono, and A. U. Siahaan, "Encryption of DES Algorithm in Information Security", International Journal for Innovative Research In Multidisciplinary Field, Vol. 4, No. 10, 2018, pp. 264 -274.

[19] Guidelines on cryptographic algorithms usage and key management, Brussels: European Payments Council (EPC) AISBL, 2021.

[20] Rasna, I. Matdoan, and S. N. Alam, " Comparison of Security Signing Data Authentication Integrity in Combination of Digest And AES Message Algorithm ", International Journal of Informatics and Information System, Vol. 4, No. 1, 2021, pp. 1 -12.

[21] A. Purwinarko, and W. Hardyanto, " A Hybrid Security Algorithm AES and Blowfish for Authentication in Mobile Applications ", Scientific Journal of Informatics, Vol. 5, No. 1, 2018, pp. 76 -80.

[22] Cloud Computing and Security Research at UbiSeC Lab (University at Buffalo), "Privacy-assured and Effective Cloud Data Utilization," Cloud Computing and Security Research at UbiSeC Lab. [Online]. Available: https://ubisec.cse.buffalo.edu/cloud/research2.html. [Accessed: Apr. 10, 2021].

[23] Cloud Computing and Security Research at UbiSeC Lab (University at Buffalo), "Scalable and Owner-controlled Cloud Data Sharing," Cloud Computing and Security Research at UbiSeC Lab. [Online]. Available: https://ubisec.cse.buffalo.edu/cloud/research3.html. [Accessed: Apr. 15, 2021].

[24] Cloud Computing and Security Research at UbiSeC Lab (University at Buffalo), "Secure Data Computation Outsourcing in Cloud," Cloud Computing and Security Research at UbiSeC Lab. [Online]. Available: https://ubisec.cse.buffalo.edu/cloud/research4.html. [Accessed: Apr. 25, 2021].

[25] S. Phatangare, G. M. Bhandari, and Y. Sharma, " New Algorithms for Secure Outsourcing of Large-Scale Systems of Linear Equations ", International Journal of Innovative Technology and Exploring Engineering, Vol. 9, No. 5, 2020, pp. 545 -550.

[26] C. Wang, K. Ren and J. Wang, " Secure Optimization Computation Outsourcing in Cloud Computing: A Case Study of Linear Programming ", IEEE Transactions on Computers, Vol. 65, No. 1, 2016, pp. 216 -229.

[27] A. Venkatesh, and M. S. Eastaff, " A Study of Data Storage Security Issues in Cloud Computing ", Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol. 3, No. 1, 2018, pp. 1741 -1745.