A Survey on Cloud Storage System Security via Encryption Mechanisms

Wejdan Alsuwat[1] and Hatim Alsuwat [1]
S44380308@st.uqu.edu.sa Hssuwat@uqu.edu.sa
[1] Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Saudi Arabia

Summary
Cloud computing is the latest approach that is developed for reducing the storage of space to store the data and helps the quick sharing of the data. An increase in the cloud computing users is observed that is also making the users be prone to hacker's attacks. To increase the efficiency of cloud storage encryption mechanisms are used. The encryption techniques that are discussed in this survey paper are searchable encryption, attribute-based, Identity-based encryption, homomorphic encryption, and cloud DES algorithms. There are several limitations and disadvantages of each of the given techniques and they are discussed in this survey paper. Techniques are found to be effective and they can increase the security of cloud storage systems.

Keywords:
Cloud Storage, Cloud Security, Cloud Infrastructure, Cloud encryption, Limitations, and Advantages.

1. Introduction

Cloud computing is the most recent solution for reducing the usage of additional resources for data storage within computer systems. A sharing environment is created between the cloud user and the cloud storage. Cloud users can release themselves due to the weight of a vast amount of data. According to the research, cloud computing can provide a centralized pool of configurable resources i.e. applications, storage, services, etc [1]. This can be released with the interaction of service providers or the minimum effort of the management.

Cloud computing is defined by the National Institute of Standards and Technology (NIST) as having five characteristics [2]. These components include the rapid expansion or elasticity of broad network access, measured service, on-demand self-service, and resource pooling. Cloud computing is considered dynamic and it is extended easily to provide transparent resources to the users over the internet [3].

There are several types of services that are offered in terms of cloud computing. The major three types of cloud computing include SaaS, PaaS, and IaaS. Software as a Service is referred to as SaaS, Platform as a Service is referred to as PaaS, and Infrastructure as a service is referred to as IaaS, [4].

There is a total of four developments models that are dependent on the requirements of the customers and these include the public cloud, community cloud, hybrid clouds, and private clouds. The physical infrastructure that is controlled and owned by the service provider is included in the public cloud. The private clouds are the infrastructure that is managed and owned by specific organizations, whereas the hybrid cloud is what includes the combination of the previous three models [5].

However, there are several cloud security categories that are studied for handling issues related to cloud security. These categories include but are not limited to security standards, network category, access control, cloud infrastructure, and the data category [6]. There are specific issues that are discussed in different categories for instance; the access control category allows the capturing of issues that impact the user information privacy and storage of data whereas the data category includes the issues that are associated with data confidentiality, integrity, migration, and data warehousing [6].

Access control challenges, cloud security standards concerns, cloud network security difficulties, data security issues, and cloud infrastructure issues are all examples of cloud security issues and categorization.

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.26

2. Searchable Encryption

At a high level, the searchable encryption system assists in encrypting the search index so that the contents are concealed from the person who is provided the proper and necessary tokens [7]. In a precise way, the search index generated for some files is encrypted in such a way that a token is given for a keyword that may obtain the file pointers that are encrypted that have the keyword, and without the token, there would be the hidden index. The generation of the token is done through the understanding of the secret key and the retrieval procedures reflect nothing about files or the keywords except for the files that have the common keyword.

There are several sorts of searchable encryption methods, each of which is tailored to certain contexts and uses. Data processors in small and consumer enterprise systems, for example, may be built using searchable encryption (SSE), whereas data processors in large business structures might be built with asymmetric searchable encryption (ASE)[7].

2.1 Symmetric Searchable Encryption

In any situation where the entity searching for data is also the one generating it, symmetric searchable encryption is applicable. The Symmetric Searchable there are several advantages of SSE and these include security and efficiency where the major disadvantage is its functionality [8]. The SSE schemes are considered efficient for both parties i.e. the one that is doing the party and the party that is performing the research. Because most SSE systems employ symmetric primitives such block pseudo-random functions and block ciphers, the encryption is deemed efficient. The security guarantees following SSE that are given as

Without any token, there is nothing learned by the servers except the length of the data. If the token is given for the keyword w, then the servers learn about the encrypted documents without learning that its w.

As the security is guaranteed stronger than the one that is provided by the asymmetric and efficiently searchable encryptio [9].

There are also disadvantages associated with the SSE are associated with the functionality and efficiency. There are different schemes that are provided by different researchers such as Curtmola et al and Goh. However, these schemes are unable to manage searches that are put together of disjunction or conjunctions of terms. Only an SSE approach based on elliptic curve pairings can tackle this problem, and it is expensive compared to other asymmetric searchable encryption [9]. Another drawback of searchable encryption structures is that they are only thought of as secure when the production of questions is done non-adaptively, that is, without taking into account the responses to prior inquiries.

2.2 Asymmetric Searchable Encryption

ASE is regarded acceptable in a variety of situations when the party searching the internet is not the same as the person creating it. We called this scenario MWSR, which stands for numerous writers/single readers. The ASE schemes are presented in several studies, and they have been much improved in recent studies [10].

Many efforts, such conjugative searches and queries range, In the public-key case, we've shown how to perform more complex search queries. Other concerns linked to the use of asymmetric searchable encryption in real systems are investigated in many studies, followed by robust ASE solutions that ensure comprehensive privacy inquiries [11].

The benefits of ASE are that if there are no tokens, The server will only learn the length of the data, and if a token for the keyword b is provided, the server will learn all encrypted documents that include that word. Efficient ASE (ESE) are well-suited to any case in which the party doing the internet search differs from the generation party and it is hard to guess. This issue is also addressed in the MWSR scenario [12]. These ESE schemes are also discussed in different researches

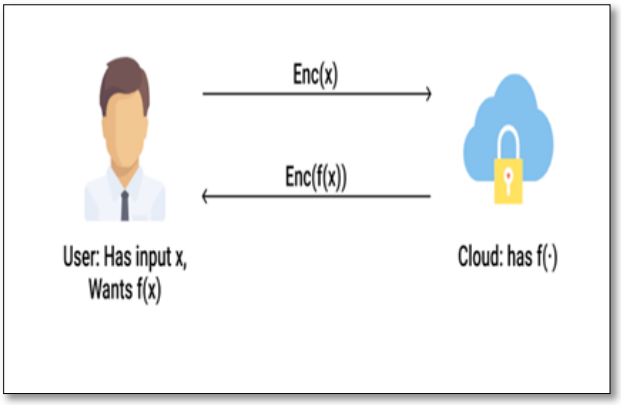
The ESE has the disadvantage of being vulnerable to dictionary attacks; in specifically, dictionary threats against the ESE may be performed directly on the encrypted index, rather than through the token, as with the ASE.

The multiuser SSE or mSSE schemes are suitable for any situations in which multiple parties desire to accept data generated by multiple parties. SWMR or single writer/many readers [13] are examples of circumstances. The token creation in this approach can be done index is encrypted, but the data owner may also revoke or add users and take privilege over his data.

3. Homomorphic Encryption

The homomorphic encryption techniques allow the users for operating cipher text indirect way. When the resultant cipher is decrypted it comes same as the operations are carried over the plaintext. Thus making use of this encryption type assures that the data of the customer is secure in all conditions that are the transmission, storage, and processing.
The homomorphic encryption idea in general is depicted in the sample image given below(1) .
The illustration depicts a basic method in which the user may add two numbers, 10 and 15, that are encrypted and saved on a cloud data server, and this presupposes that the numbers will not be modified e.g. 10 is changed to 100 and 15 is changed to 150. So, the impact on the total calculation would also occur. When the data is decrypted, it is again converted to the original values and the original results get visible[14]. This type of encryption can be divided into partial or fully homomorphic encryption. On the ciphertext, the FHE enables both addition and multiplication. This allows the user to do encrypted searches on the internet. In this process, the input is sent in encrypted form and the user sends it to the search engine that handles multiple multiplications and addition to the ciphertext and then returns the decrypted search results [15]. The first fully homomorphic encryption was done in 2019 and before that partial homomorphic encryption. However, the major issue with the partial homomorphic encryption system includes either multiplication operations or multiplication operations. This means that the partial homomorphic encryption schemes can either perform single multiplication with multiplication[16].

Another cryptosystem known as the Paillier cryptosystem scheme is considered a homomorphic encryption scheme that gives support to the addition operation.
Homomorphic encryption is the new concept that allows the users for operating encrypted data so it seems to be the solution to the problem of data security.



Figure(1): Technique Of Encryption using Homomorphism

4. Identity-Based Encryption

Identity cryptography based on was developed in 1984 by Shamir. It's a traditional method for encrypting texts. The fact that this encryption scheme is based on RSA is a serious flaw. Other specialists identified as Franklin and Boneh [17] established efficient identity-based encryption later in 2001.
The identity of the user plays a key role in identity-based encryption systems. In order to send encrypted communications, the sender must know the identity of the receiver. The most common use for determining identity-based encryption is email encryption. However, this identity-based encryption does not allow for key revocation. There are different researches that explain this type of system. This protocol is more efficient and lightweight than other protocol[18].

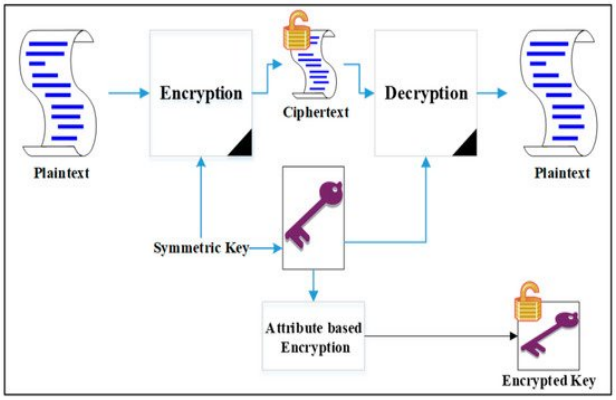
5. Attribute-based Encryption

ABE is a novel public key encryption approach that operates in a variety of ways. Fuzzy encryption is another name for this sort of encryption. . The public key encryption methods are used for encrypting data over the servers of third parties while distributing decryption keys for authorizing users as shown in figure(2) [19]. The drawbacks to public-key encryption include the difficulty to efficiently manage distribution keys, lack of scalability and flexibility, and the need of the owner to be online whenever there is encryption or decryption of the data. ABE minimizes is the solution to all such problems and it can reduce the communication overhead of the internet increase flexibility, scalability, and gain fine access control for systems present at a large scale [20]. ABE is used to deal with DAC, MAC, RBAC, and ABAC, among other classic access control techniques. There are various features and limitations of different schemes. The limitations of these techniques are the possibility to conflict with the original message, Role explosion, restricted user capabilities, significant administrative costs and the organizational changes that are required for managing attributes [21].

However, the complete analysis of ABE shows it to be an extensively useful technique for accessing the control in cloud computing and allows key strength. The major ABE techniques that can be considered are given are given as
ABE; The technique uses the attributes as the identities of both decryption or encryption of data. The ciphertext and the secret user key depend on attributes in this case. If the attributes are matched with the ciphertext then decryption is allowed[22]. There are a set of four algorithms that are used in this technique and there are limitations to this technique too. The first is an absence of ability to express threshold values and the second is the presence of different user categories for creating a computational overhead [23].

The security settings are set up to use PK to encrypt the message M and descriptive property S for producing the Cipher Text in Key Policy ABE, which is a modified variant of basic ABE presented (CT). The user is given the KP-ABE policy, which provides preliminary assistance in preserving factors such as secrecy, revocation, accountability, collision resistance, and secure access control [24].

Key Policy ABE, Ciphertext Policy ABE, Expressive Key Policy ABE, Ciphertext Policy Hierarchical Identity-Based Encryption, and Attribute-Set-Based Encryption are all examples of ABE encryption.



Figure(2) : Technique Of Attribute-based Encryption

6. Cloud DES Algorithm

This data security idea is a smart way to improve data security in cloud computing by employing the DES algorithm. This technique is thought to be the best for both client and server security. The DES encryption block chaining was created to eliminate data storage fraud. The data that is transmitted to the compromised receiver can be replaced without risk. The system connected with encryption is regarded safe, although the type of encryption that is strengthened is proportionate to the computer's power [25]. There is also the usage of a symmetric key that is more effectively employed for model encryption. Cloud data security, data security risk, data security procedures, and security functions of data deployment are all well-covered in this system. This method may ensure that the entire process is enhanced by implementing a comprehensive security solution [26].

Another encryption algorithm has been discussed in another paper that deals well with the issue of privacy and data security. There are two kinds of assaults of which the data is able to store in the cloud and these include the insider attack and outsider attack. The insider attack can be made through the admin of an organization who has the privilege of accessing the created user data whereas the outside

attack is the attack by the third party who is trying to access the data [28]. The researchers propose the symmetric encryption algorithm for guarding the data to protect the data from external attacks. The general working of this technique is to convert the plain text to the ciphertext using the ASCII code and then assign the key values from 1 to 256 to the data. With the combination of the substitution, the traditional technique's effectiveness is increased. The symmetric encryption results in the formation of computational efficiency and more speed for handling a large amount of data. This algorithm doesn't allow hackers or even administrators to access the data type from the cloud storage as the user data is encrypted. There are several algorithms that are based

7. Discussion

The structural design associated with cloud computing creates the security of data because of some techniques and users may find difficulties related to the data to be shared over the cloud storage over the internet.

There are numerous benefits of cloud computing in society but there are several risks factors associated with it too. The major issues that are also discussed in this paper are the privacy protection and security of data, access control, authentication of users, and application security. There are various techniques that are discussed in this paper related to securing data and increasing the confidentiality and integrity of data. Control access and User control are highly discussed issues in cloud computing.

The security of the data is the main concern of all companies. Hackers are found to breach most of the previous security mechanisms for cloud computing. There are various encryption techniques that are discussed in this survey paper that enables single users and corporates to secure their data over the cloud.

It was also found that simple encryption is not the reliable way to secure the data but there are different combinations of security techniques that are discussed in this paper.

8. Conclusion & Future work

The research shows that there are several cloud storage encryption mechanisms that can be implemented in different settings. There are both pros and cons of each of the approaches but it's important to determine what level of encryption is required to perform the task well in a specific setting. Different encryption techniques are observed in this paper and this shows that a lot of work has been done for proposing the cloud storage encryption mechanisms. However, the data is required to be protected and a secure system must be established based on the above-given encryption techniques. It is also observed from the analysis that not all techniques are suitable for each situation but this is also a good sign that a large number of encryption techniques are given that are not even discussed in this survey paper. Cloud is the future generation storage essential and it must be secure to increase the people's confidence to use cloud services without being feared of their data being hacked. Overall this survey paper elaborates the major techniques and helps the cloud developers and users to select the best fir cloud security encryption technique to increase the security, privacy, and fast transfer of data.

References

[1] S. Ashwini, "(PDF) Research Paper on Cloud Computing," ResearchGate. https://www.researchgate.net/publication/352477780_Research_Paper_on_Cloud_Computing (accessed Mar. 18, 2022).

[2] G. Novkovic, "Control Engineering | Five characteristics of cloud computing," Control Engineering, Aug. 11, 2017. http://blog.mesa.org/2017/08/manufacturing-in-cloud-part-ii-5.html (accessed Mar. 18, 2022).

[3] Y. Cai, W. Lu, L. Wang, and W. Xing, "Cloud Computing Research Analysis Using Bibliometric Method," Int. J. Soft. Eng. Knowl. Eng., vol. 25, no. 03, pp. 551–571, Apr. 2015, doi: 10.1142/S0218194015400203.

[4] M. Ramzan, M. S. Farooq, A. Zamir, W. Akhtar, M. Ilyas, and H. U. Khan, "An Analysis of Issues for Adoption of Cloud Computing in Telecom Industries," Engineering, Technology & Applied Science Research, vol. 8, no. 4, Art. no. 4, Aug. 2018, doi: 10.48084/etasr.2101.

[5] S. U. Khan, H. U. Khan, N. Ullah, and R. A. Khan, "Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach," Security and Communication Networks, vol. 2021, p. e1024139, Sep. 2021, doi: 10.1155/2021/1024139.

[6] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, vol. 4, no. 1, p. 5, Feb. 2013, doi: 10.1186/1869-0238-4-5.

[7] S. .R and C. Banupriya, "A SURVEY ON CRYPTOGRAPHIC CLOUD STORAGE TECHNIQUES," Oct. 2020, doi: 10.5281/zenodo.829787.

[8] G. Wang, C. Liu, Y. Dong, P. Han, H. Pan, and B. Fang, "IDCrypt: A Multi-User Searchable Symmetric Encryption Scheme for Cloud Applications," IEEE Access, vol. 6, pp. 2908–2921, 2018, doi: 10.1109/ACCESS.2017.2786026.

[9] Y. Wang, J. Wang, and X. Chen, "Secure searchable encryption: a survey," J. Commun. Inf. Netw., vol. 1, no. 4, pp. 52–65, Dec. 2016, doi: 10.1007/BF03391580.

[10] C. Bösch, P. Hartel, W. Jonker, and A. Peter, "A Survey of Provably Secure Searchable Encryption," ACM Comput. Surv., vol. 47, no. 2, p. 18:1-18:51, Aug. 2014, doi: 10.1145/2636328.

[11] M. I. Salam et al., "Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage," Human-centric Computing and Information Sciences, vol. 5, no. 1, p. 19, Jul. 2015, doi: 10.1186/s13673-015-0039-9.

[12] J. Li, X. Niu, and J. S. Sun, "A Practical Searchable Symmetric Encryption Scheme for Smart Grid Data," arXiv:1808.00645 [cs], Oct. 2018, Accessed: Mar. 18, 2022. [Online]. Available: http://arxiv.org/abs/1808.00645

[13] S. U. Khan, H. U. Khan, N. Ullah, and R. A. Khan, "Challenges and Their Practices in Adoption of Hybrid Cloud Computing: An Analytical Hierarchy Approach," Security and Communication Networks, vol. 2021, p. e1024139, Sep. 2021, doi: 10.1155/2021/1024139.

[14] K. S. Kim, M. Kim, D. Lee, J. H. Park, and W.-H. Kim, "Forward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas Texas USA, Oct. 2017, pp. 1449–1463. doi: 10.1145/3133956.3133970.

[15] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Jan. 2010, pp. 136–149. doi: 10.1007/978-3-642-14992-4_13.

[16] B. Vankudoth, "(PDF) Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey," ResearchGate, doi: 10.5120/ijca2017913063.

[17] G. Yang, "Homomorphic Encryption Technology for Cloud Computing," Procedia Computer Science, vol. 154, pp. 73–83, Jan. 2019, doi: 10.1016/j.procs.2019.06.012.

[18] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation," arXiv:1704.03578 [cs], Oct. 2017, Accessed: Mar. 19, 2022. [Online]. Available: http://arxiv.org/abs/1704.03578

[19] Y.-F. Tseng and C.-I. Fan, "Anonymous Multireceiver Identity-Based Encryption against Chosen-Ciphertext Attacks with Tight Reduction in the Standard Model," Security and Communication Networks, vol. 2021, p. e5519721, Jun. 2021, doi: 10.1155/2021/5519721.

[20] P. H. D, "Identity-Based Cryptography and Comparison with traditional Public key Encryption: A Survey."

[21] N. Chaudhari, M. Saini, A. Kumar, and P. Govindaraj, "A Review on Attribute Based Encryption," Dec. 2016, pp. 380–385. doi: 10.1109/CICN.2016.81.

[22] F. Meng, L. Cheng, and M. Wang, "Ciphertext-policy attribute-based encryption with hidden sensitive policy from keyword search techniques in smart city," EURASIP Journal on Wireless Communications and Networking, vol. 2021, no. 1, p. 20, Feb. 2021, doi: 10.1186/s13638-020-01875-2.

[23] M. U. Aftab et al., "Traditional and Hybrid Access Control Models: A Detailed Survey," Security and Communication Networks, vol. 2022, p. e1560885, Feb. 2022, doi: 10.1155/2022/1560885.

[24] B. Jayant.D, U. A, A. S, and M. G, "Analysis of DAC MAC RBAC Access Control based Models for Security," International Journal of Computer Applications, vol. 104, pp. 6–13, Oct. 2014, doi: 10.5120/18196-9115.

[25] D. Chang, W. Sun, Y. Yang, and T. Wang, "A Dynamic Access Control Method for SDN," Journal of Computer and Communications, vol. 7, no. 10, Art. no. 10, Oct. 2019, doi: 10.4236/jcc.2019.710010.

[26] M. Basri, H. Mawengkang, and E. M. Zamzami, "Cloud Computing Security Model with Combination of Data Encryption Standard Algorithm (DES) and Least Significant Bit (LSB)," J. Phys.: Conf. Ser., vol. 970, p. 012027, Mar. 2018, doi: 10.1088/1742-6596/970/1/012027.

[27] S. Mewada, A. Sharivastava, P. Sharma, S. Gautam, and N. Purohit, "Performance Analysis of Encryption Algorithm in Cloud Computing," Nov. 2016. doi: 10.13140/RG.2.2.29836.51840.

[28] N. Al-gohany and S. Almotairi, "Comparative Study of Database Security In Cloud Computing Using AES and DES Encryption Algorithms," Journal of Information Security and Cybercrimes Research, vol. 2, Jan. 2019, doi: 10.26735/16587790.2019.004.