ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/girish-ganachari/292

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 3

Research Article

Enhancing Data Privacy in AWS S3: A Comparative Analysis of Encryption Algorithms and Access Control Mechanisms

Girish Ganachari*

Citation: Ganachari G. Enhancing Data Privacy in AWS S3: A Comparative Analysis of Encryption Algorithms and Access Control Mechanisms. *J Artif Intell Mach Learn & Data Sci 2023*, 1(3), 1281-1284. DOI: doi.org/10.51219/JAIMLD/girish-ganachari/292

Received: 02 September, 2023; **Accepted:** 18 September, 2023; **Published:** 20 September, 2023

***Corresponding author:** Girish Ganachari, USA, E-mail: girish.gie@gmail.com

ABSTRACT

This paper aims to compare the strengths of various encryption algorithms and the access control methods in AWS S3. One important factor in the use of cloud storage is data privacy and security whenever there is an investment in cloud storage. Based on an analysis of various encryption techniques as well as the various modes of client-oriented access control methods, this paper offers blueprints for the best practices of data security in AWS S3.

Keywords: AWS S3, Data Privacy, Encryption Algorithms, Access Control Mechanisms, Cloud Security

1. Introduction

Cloud preservation has become a crucial topic in current research since many organisations share their data in cloud storage systems. AWS S3 commonly known as Amazon Simple Storage Service is one of the most popular cloud-based storage solutions providing Storage as a Service. However, there is a security issue when storing data through AWS S3. This paper seeks to discuss several encryption algorithms and several access control measures to increase S3 data privacy in AWS.

2. Literature Review

A. Cryptographic Methods

A comparative evaluation of various forms of cryptographic techniques adopted by cloud service suppliers with a special focus on the relevance of encryption as a shield in data protection[1]. Different methods of data security and privacy preservation for cloud storage, where encryption is found to be a prominent solution[2].

Homomorphic encryption can be applied to protect data privacy in clouds as computations can be made on the encrypted database without the need to decrypt them[11]. One technique of applying data privacy can be performed with the use of symmetric cryptographic algorithms that establish the efficiency of such methods in protecting cloud data stored on other servers[12].

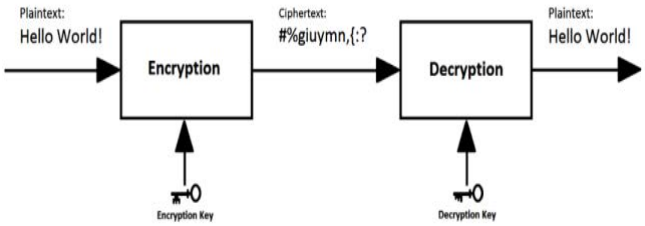

Figure 1: Cryptographic Technique.

B. Access Control Mechanisms

Security measures are a critical component that is required to implement in implement cloud environment specifically AWS S3. Although RBAC is a simple solution for user permission, it is the same as the previous one and involves roles, it implies overprivileged users[11]. Attribute-Based Access Control (ABAC) is more refined than the previous models; focuses on user attributes as well as resource characteristics to set the access

privilege of a user, which makes it more secure[12]. The client-centric approach of access control entails making data encrypted on the client side and only the permitted client can decrypt the data which means more security[1] 3. The method of access control with an emphasis on the client is an effective way to increase cloud security[24].

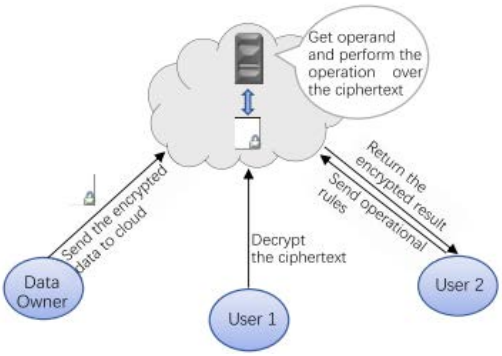

Figure 2: Homomorphic Encryption.

The issue of security vs. convenience in the context of a/c and its frameworks[13]. A form of encryption, attribute-based encryption (ABE) with multiple benefits for the secure access of data[13]. Altogether these mechanisms considered some security issues in AWS S3 according to the literature.

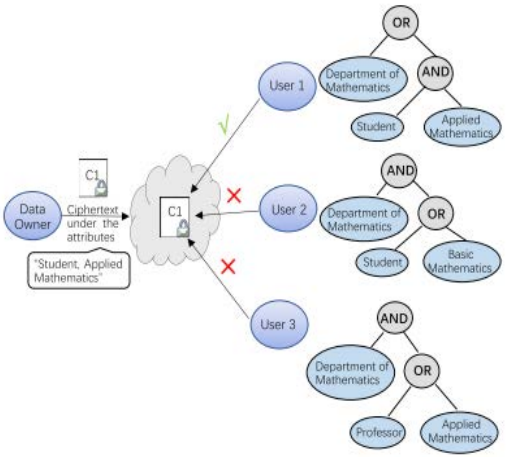

Figure 3: ABE.

3. Methodology

A. Encryption Algorithms

In the method, the authors have compared various encryption algorithms based on their security measures, computational capability, and simplicity considering numerous research articles.

***Advanced Encryption Standard (AES)*:** AES is well known to be highly secure and also efficient which is a huge benefit. It employs the use of symmetric key encryption, which despite being quite efficient in terms of computation, is, however, closely associated with key management issues that if not managed properly, can lead to compromised security. AES is used in those applications that require higher performance because the computing overhead of AES is low[12].

***Rivest-Shamir-Adleman (RSA)*:** RSA is a criterion of symmetric encryption key distributing high security through public and private keys. Although it provides good security, it is rather slow, and thus not recommended for real-time scenarios[6]. RSA is used commonly for the encryption of data and the distribution of the keys[8].

***Attribute-Based Encryption (ABE)*:** In ABE, optional attributes can be tied with a Key so that the number of access conditions can be controlled precisely[8]. This also offers flexibility in the policies of access control since a complex policy can easily be implemented, and the security of the data is boosted since only people with correct attributes in the equation can decrypt the data.

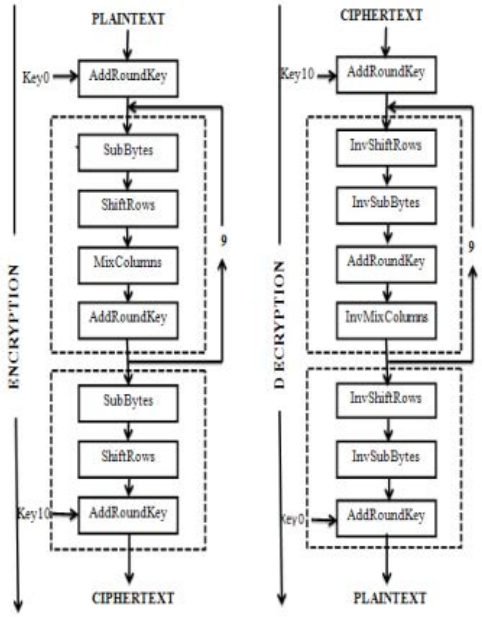

Figure 4: AES.

B. Access Control Mechanisms

The methodology reviews several emphasis points whereby different kinds of access controls used in AWS S3 are uniformly assessed concerning the security strength of the access control measure, usability and implementation to a large extent from the literature.

***Role-Based Access Control (RBAC)*:** RBAC distributes permissions based on the user roles, thus easy to manage and no overhead in control. On the other hand, the authors found that when roles are not well controlled, the system can end up with overprivileged users[21]. RBAC works well where there is a clear role hierarchy and clear definitions of permissions[15].

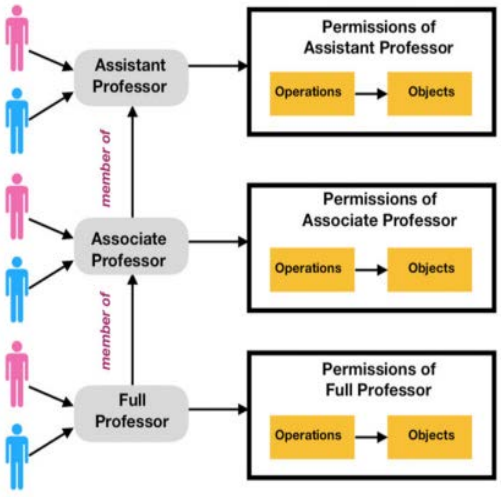

Figure 5: RBAC.

***Attribute-Based Access Control (ABAC)*:** Due to its utilization of characteristics such as user characteristics and type of a resource as its basic control parameter, ABAC finally offer fine-grained access control[7]. It also improves security in a way that provides the flexibility of gaining access according to many factors, yet at the same time provides secure and specific control[20,23]. ABAC is most appropriate in environments that are constantly changing since access requirements are also frequently changing[10,18].

***Client-Centric Access Control*:** This mechanism involves encrypting data at the client level to make sure that only those clients should be able to decrypt the said data[18]. This approach improves security by ensuring that the data in transit as well as the data at rest is encrypted all the time[6]. This type of access control is good if end-to-end security is essential, especially for the clients.

4. Analysis and Results

A. Performance Evaluation

Assessing the performance of the encryption algorithms, it is clear that AES has the least overhead and is thus recommended where performance is key. Relatively, RSA provides high security compared to the other two while it is more resource-consuming and thus not very appropriate for real-time use[9]. Attribute-based encryption allows much more flexible and precise access control of the encrypted contents but the attribute management should be done precisely[10]. Another disadvantage of RSA draws focus on the high computational costs of modern RSA in cloud computing[15]. Proper encryption mechanism to avoid them being a performance degrader[22].

B. Security Assessment

The security analysis of encryption algorithms reveals that AES, RSA and ABE have good security in guarding AWS S3. These algorithms' effectiveness is highly dependent on the key management practices that have been adopted. AES is highly secure and it incurs small computational costs so it is appropriate for a whole lot of applications[9]. RSA although very secure, needs to manage keys in a very efficient manner due to the use of asymmetric keys[4]. ABE also guarantees a more precise level of access control; moreover, increased safety is achieved when attributes are linked to the data encryption keys[7]. Encryption and access control measures should be well-initially put in place and implemented for successfully eliminating security threats in cloud environments[17]. Furthermore, the significance of the key management is to keep the data safe[10].

5. Implementation in AWS S3

AWS S3 offers different encryption models such as SSE and CSE where the above statement is partially correct because AWS S3 provides SSE and other encryption models not mentioned in the statement. SSE enables the AWS to manage the encryption keys; while this facilitates key management, it reduces the ownership since it is trusted by the AWS[19]. On the other hand, CSE allows clients to retain key control all the time and this provides the greatest security though the management may be slightly complicated[25].

A. Server-Side Encryption (SSE)

AWS S3 provides several features for server-side encryption (SSE) for the purpose of increasing the scope of security. SSE-S3 entails the aspect where AWS holds the keys to the encryption; they are easy to use, and data is well protected. SSE-KMS exploits AWS Key Management Service (KMS) to perform key management and provides extra security features and audited logs [5]. The capabilities of SSE-C comprise the opportunity for customers to transmit their keys for encryption which means the ultimate control of the process[14,16].

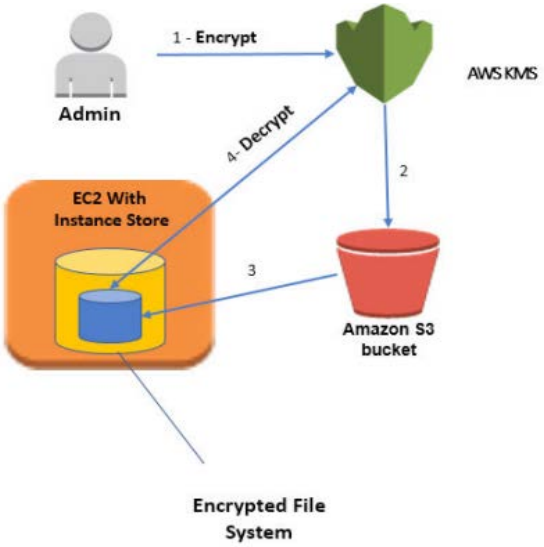

Figure 6: Encrypted File System.

B. Client-Side Encryption (CSE)

AWS S3 CSE enables customers to encrypt data in their client application before uploading to S3, which means data is encrypted at customers' sites and throughout the lifecycle of data in S3. This means is a lot more secure as the keys for the encryption are not held by AWS but instead, it is held by the client[10,14]. This approach is particularly beneficial for raw data as it incorporates various levels of keys for purposed data extraction hence only the authorized personnel can obtain the sensitive data[7,12]. CS encryption also improves data security since the users' data cannot be accessed by third parties during transmission and storage[20]. This method also helps to decrease risks connected with server-side vulnerabilities as well as possible breaches at the level of the service provider[19,22].

6. Conclusion

This paper's findings suggest that AWS S3 is best encrypted with AES and that ABAC and client-centric access control methods offer the highest levels of security. This approach explains how client-side encryption helps to solve various issues related to data security at the different stages of the data life cycle. In cryptography, often is said that key management is half the battle which implies that managed keys are secure keys. Therefore, future research should concentrate on the option of automating key management for client-side encryption. This paper therefore establishes a correlation between the efficiency of the encryption algorithms and access control mechanisms to improve on the data privacy in cloud storage systems.

7. References

1. Sudha, D., 2020. Data Security in cloud service providers-a Comparison of different cryptographic methods.
2. Adjei, A., Ofori, F., Birago, B. and Ofori, I., 2018. Enhancing security in the cloud using encryption in a client centric access control mechanism. *Br. J. Comput. Netw. Inf. Technol.*, *1*(1), pp.19-48.

3. El Sibai, R., Gemayel, N., Bou Abdo, J. and Demerjian, J., 2020. A survey on access control mechanisms for cloud computing. *Transactions on Emerging Telecommunications Technologies*, *31*(2), p.e3720.
4. Reddy, P.P. and Reddy, N.A., 2022. Amazon Web Services Provides Dual Access for Cloud-Based Data Storage and Sharing.
5. Yang, P., Xiong, N. and Ren, J., 2020. Data security and privacy protection for cloud storage: A survey. *Ieee Access*, *8*, pp.131723-131740.
6. Kaaniche, N. and Laurent, M., 2017. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications*, *111*, pp.120-141.
7. Backes, J., Bolignano, P., Cook, B., Dodge, C., Gacek, A., Luckow, K., Rungta, N., Tkachuk, O. and Varming, C., 2018, October. Semantic-based automated reasoning for AWS access policies using SMT. In *2018 Formal Methods in Computer Aided Design (FMCAD)* (pp. ٩-١). IEEE.
8. Gupta, L.M., Garg, H. and Samad, A., 2022. A Secure Data Transfer Approach With an Efficient Key Management Over Cloud. *International Journal of Information Technology and Web Engineering (IJITWE)*, *17*(1), pp.1-21.
9. Khuntia, S., Krishna, D. and Sahay, S., 2021. Secure Attribute-based User Access Control over AWS Cloud. *IJRASET*, *9*(2), pp.7-33.
10. Rath, A., Spasic, B., Boucart, N. and Thiran, P., 2019. Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and Azure. *Computers*, *8*(2), p.34.
11. Murthy, S. and Kavitha, C.R., 2019, June. Preserving data privacy in cloud using homomorphic encryption. In *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. ١١٣٥-١١٣١). IEEE.
12. Livingston, D., Kirubakaran, E. and David, E.P., 2021. Implementing Data Privacy of Cloud Data on a Remote Server using Symmetric Cryptographic Algorithms. *International Journal of Advances in Data and Information Systems*, *2*(1), pp.62-72.
13. Mittal, A., 2017. Attribute based encryption for secure data access in cloud.
14. Kewate, N., Raut, A., Dubekar, M., Raut, Y. and Patil, A., 2022. A review on AWS-cloud computing technology. *International Journal for Research in Applied Science and Engineering Technology*, *10*(1), pp.258-263.
15. Bharathan, T. and Kumar, B.S., 2019. Implementing information security mechanism over cloud network. *Int. J. Recent Technol. Eng*, *8*(2), pp.1706-1710.
16. Park, S.J., Lee, Y.J. and Park, W.H., 2022. Configuration method Of AWS security architecture that is applicable to the cloud lifecycle for sustainable social network. *Security and Communication Networks*, *2022*(1), p.3686423.
17. Mishra, A. and Kumar, G., 2021. Big Data Analytics on AWS Cloud. *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, *10*(04).
18. Talha, M., Sohail, M. and Hajji, H., 2020. Analysis of research on amazon AWS cloud computing seller data security. *International Journal of Research in Engineering Innovation*, *4*(3), pp.131-136.
19. Mushtaq, M.S., Mushtaq, M.Y., Iqbal, M.W. and Hussain, S.A., 2022. Security, integrity, and privacy of cloud computing and big data. In *Security and privacy trends in cloud computing and big data* (pp. ٥١-١٩). CRC Press.
20. Kayode, O., 2020. A cloud based approach for data security in IoT. *Comput. Eng. Intel. Syst.*, *11*, pp.16-23.
21. Dashti, W., Sajid, A., Jahangeer, A. and Zafar, A., 2020. Security challenges over cloud environment from service provider prospective. *Cloud computing and data science*, pp.12-20.
22. Continella, A., Polino, M., Pogliani, M. and Zanero, S., 2018, December. There's a hole in that bucket! a large-scale analysis of misconfigured s3 buckets. In *Proceedings of the 34th Annual Computer Security Applications Conference* (pp. ٧١١-٧٠٢).
23. Latha, D.P.P., Pushparaj, D.J. and Helina, S.T., 2022. An Efficient Approach of Security Risk Mitigation in Cloud. *Journal of Pharmaceutical Negative Results*, pp.338-342.
24. Challa, N., Devineni, S.K. and Karangara, R., 2022. A deep dive into amazon web services: Unlocking the potential. *Journal of Artificial Intelligence & Cloud Computing*, *1*, pp.2-5.
25. Kumar, N.G., Polala, N. and Kumari, D.A., 2017. Enhanced Methods to Provide Privacy from Massive Surveillance. *Indian Journal of Science and Technology*, *10*(6).