International Journal of Research in Engineering, Science and Management
Volume 6, Issue 5, May 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Dual Access Control for Cloud based Data Storage and Sharing Using AES Algorithm

Rajesh Thanikachalam[1], Devesh Balakrishnan[2], Vedantham P. S. Srinivasa Iyengar[3*], Prabhat Kumar[4]

[1,2,3,4]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India

***Abstract*: The green and lower priced management of cloud-primarily totally based facts garage has attracted developing hobby from academia and industry in recent years Since offerings are brought over an open network, it's miles vital for carrier carriers to use secure data storage and sharing mechanisms to protect user privacy and the confidentiality of data. The most well-known method for preventing the compromise of sensitive information is encryption. The real necessity for statistics management, however, can't be absolutely met with the aid of using merely encrypting statistics (for instance, the usage of AES). Additionally, a robust get right of entry to manage over download requests should be taken into consideration to save you Economic Denial of Sustainability (EDoS) attacks from being launched to prevent clients from using the service. In this research, we discover twin get right of entry to manage withinside the context of cloud-primarily totally based storage, withinside the experience that we construct a manage mechanism over each statistics get right of entry to and download requests without sacrificing safety or efficiency. This paper presents the format of dual get proper of access to control systems, one for each intended environment. Additionally, the systems' experimental evaluation and safety are presented.**

***Keywords*: AES, EDoS, Cloud, Storage, Confidentiality.**

1. Introduction

In this research, we provide a completely unique privacy-keeping technique for public auditing of shared cloud data. We are using ring signature to get the verification information required to verify the validity of shared data. Our approach ensures that the identity of the signer for each block in shared data remains undisclosed to public verifiers. Through this method, verifiers can efficiently verify the integrity of shared data without the need to request the entire file. Furthermore, instead of individually verifying each auditing task, our mechanism is capable of simultaneously performing multiple auditing tasks.

The suggested solution is a public auditing tool for cloud-shared data that protects privacy. Our method builds homomorphic authenticators using ring signatures, allowing a public verifier to evaluate the privacy of shared data without needing access to the complete dataset. The verifier, however, is unable to determine who signed each data block specifically. We have improved our method to handle batch auditing, enabling the effective verification of several auditing jobs concurrently, which will significantly increase efficiency.

One of them is traceability, which describes the group manager's ability to reveal the signer's identity based on verification information in a limited number of scenarios. AES is an unchanging alternative to the Feistel cypher. The replacement permutation network is supported. It is made up of a sequence of linked operations, some of which need exchanging insert for specified outputs and others which require shifting bits about. astonishingly, AES plays all its computations on bytes in place of bits. As an output, AES considers a decoded block's one twenty-eight bits as 16 bytes. These sixteen-byte square measurements are organized in 4 columns and four rows for use as a matrix.

A. Objective

We propose a dual access control scheme that permits for communal(public) auditing of distributed information stored in the cloud. Recent research has been conducted to support the evolution of cloud computing towards the internet of services. As an outcome of the growing popularity of cloud services, security and privacy/security problems are becoming major concerns.

2. Literature Survey

A. Existing System

The present technique introduces a brand new extreme privateness difficulty withinside the occasion of shared facts with using identification privateness leaking to public verifiers. The normal technique for verifying facts correctness is to acquire the entire facts set from the cloud after which validate facts integrity via way of means of checking signature accuracy. The following key needs have to be carried out so that you can accurately set up an powerful third party auditor (TPA): 1) TPA must be capable of unexpectedly audit cloud information garage without requiring a neighbourhood reproduction of information, implementing no greater on line fee at the cloud person; 2) The third-party auditing method must create no new dangers to person information privacy.

The paper titled "QoS Support for End Users of I/O-intensive Applications Using Auditing Shared Storage Systems," written by Xuechen Zhang from the ECE Department at Wayne State University and Kei Davison from the Alamos National Laboratory, was published in the November 2010 edition of the

*Corresponding author: vp5610@srmist.edu.in journal Parallel and Distributed Systems, with a focus on enhancing Quality of Service for end-users of input/output-intensive applications through the auditing of shared storage systems. We recall the hassle of building an erasure code for garage over a community while the facts reassets are distributed. Specifically, we expect that there are n garage nodes with confined reminiscence and okay < n reasserts producing the facts. We need a facts collector, who can seem everywhere withinside the community, to question any okay garage nodes and be capable of retrieve the facts. We introduce Decentralized Erasure Codes, which can be linear codes with a selected randomized shape stimulated via way of means of community on arbitrary bipartite graphs, coding. Decentralised erasure codes are shown to be ideally sparse and to have lower communication, storage, and computation values than random linear coding.

In December 2014, the Key Laboratory of Mathematics Mechanization published an article entitled "Repair Locality from a Combinatorial Perspective," written by Anyu Wang and Zhifang Zhang, which discusses repair locality in the context of combinatorics. Plutus is a cryptographic storage machine that permits stable report sharing without putting tons agree with at the report servers. It makes novel use of cryptographic primitives to guard and proportion files. Plutus functions extraordinarily scalable key control whilst permitting man or woman customers to maintain direct manage over who receives get entry to to their files. We give an explanation for the mechanisms which are in Plutus to lessen the wide variety of cryptographic keys that exchanged among customers via way of means of the use of report groups, distinguish report study and write get entry to take care of person revocation efficiently, and permit an untrusted server to authorize report writes. We have constructed a prototype of Plutus on Open AFS. Measurements of this prototype display that Plutus achieves robust safety with overhead corresponding to structures that encrypt all community traffic.

The promotion of A.J.C. van Gemund from the Delft University of Technology supervised the thesis of Prof.dr.ir. H.J. Sips from the same institution, titled "On the Effective Parallel Programming of Multi-core Processors," which was completed on December 7, 2010, with Prof.dr.ir. H.E. Bal also serving as a supervisor. Availability is a storage machine asset this is each fantastically preferred and but very less engineered. While many systems offer features to improve availability, such as redundancy and failure recovery, the task of effectively configuring these mechanisms is often left to the system manager. Unfortunately, most people lack the skills to manage the associated trade-offs and often lack the time to adapt these configurations to changing conditions. As a result, many systems are statically configured with limited understanding of how these configurations impact overall performance and availability. This challenge becomes even more complex in distributed or shared systems and is particularly crucial in wide-area peer-to-peer storage infrastructures. This study presents a revolutionary "Totally Recalling" peer-to-peer storage system that automates availability management. The Totally Recalling system automatically measures and calculates the availability of its host components, forecasts their availability in the future based on past behaviour, chooses the proper redundancy mechanisms and repair policies, and provides user-specific availability while maximising efficiency.

In 2010, Peter Sobs from the Institute of Computer Engineering at the University of Luebeck in Germany wrote an article entitled "Parallel Reed/Solomon Coding on Multicore Processors," which was published in the IEEE and can be accessed through DOI 10.1109/SNAPI.2010.16. This paper says the layout of previous, a big-scale, net-based, international garage application that offers scalability, excessive availability, endurance, and security. PAST is a peer-to-peer Internet software and is completely self-organising. previous node's function get admission to factor for clients, take part withinside the route of purchaser requests, and make contributions storage to the device. Nodes aren't trusted, they will be part of the device any time and might silently go away the device without warning. Yet, the device is capable of offer robust assurances, green storage get admission to, load balancing and scalability.

B. *Limitations*

- Customers' stored data is not physically in their possession, therefore conventional cryptographic techniques for maintaining data security cannot be directly used.
- They don't carry out several auditing jobs at once.
- Loss of information.
- No longer is personal information kept secret.
- The time required for authentication is too long.

3. Module Description

A. *Registration of User*

During the registration process of an individual with an identification ID, the supervisor of the organization selects a number in a random manner. This number is then included in the organization's personnel database for future reference. Following the registration, the individual is provided with a unique private key that will be used for generating organization signatures and decrypting documents.

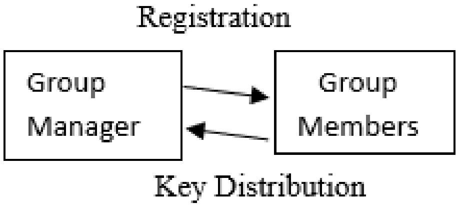


Fig. 1. User registration

B. *Auditing (Public)*

Linear authenticators refer to verification metadata that are derived from individual data blocks and can be efficiently combined in a manner that allows auditors to validate the correctness of the aggregated authenticator. To ensure privacy-preserving public auditing, our proposed approach combines the Homomorphic/linear/similar authenticator with a technique involving random masks in a unique way. In our procedure, the linear aggregate of selected data blocks in the server's response is obscured using randomness generated through a pseudo-random function (PRF). This ensures that the resulting scheme provides privacy while still enabling the verification of aggregated data blocks.

- Setup Phase
- Audit Phase

C. Data Sharing

The most prevalent use case for the application is data transfer. When efficient and flexible delegation is expected, the utility of public auditing becomes valuable. By providing a single and compact composite key to each authorized user, the approach allows a content provider to communicate their data securely and selectively, with a fixed and minimal increase in ciphertext size.

D. Integrity Check

Therefore, it is crucial to enable data dynamics while ensuring the security of public risk auditing. Here, we show how our basic architecture may be altered to allow data dynamics, including operations like block-level insertion, modification, and deletion. We can provide public risk auditing that protects privacy and supports data dynamics by including this methodology into our design. The client can download only certain parts of the file instead of the complete thing.

E. Related Work

ABE has been provided withinside the literature to offer fine-grained coverage-primarily based totally manage over encrypted statistics. ABE has principal studies branches: CP-ABE and KP-ABE, which stands for key coverage ABE. This examine specializes in the previous. In a CP-ABE, the decryption secret is connected to a characteristic set, and the ciphertext is connected to an get entry to coverage. This capability qualifies CP-ABE for secure cloud statistics exchange.

1. The term "twin get admission to control" could be used henceforth to refer to govern over encrypted statistics and down load requests. (in assessment to KP-ABE). This is due to the fact KP-ABE calls for the decryption key to narrate to the get admission to policy, which leads to excessive garage fees for cloud users. Many works were proposed to hire CP-ABE in numerous programs because the creation of seminal CP-ABE, along with responsible and traceable CP-ABE multi-authority, outsourced CP-ABE, and extendable variants.
2. Despite its cap potential to aid access to fine-grained data, using CP-ABE as a unmarried answer is a ways from sensible and powerful in protecting towards EDoS assaults [11],

As is the case with D-DoS withinside the cloud setting [11], many countermeasures to the assault were proposed withinside the literature [12], [3]. However, Xue [8] claimed that preceding works couldn't absolutely protect towards the EDoS assault on the protocol level, and that they proposed a technique to guard or protect cloud records sharing from the assault. [8] does, however, have drawbacks. To begin, in an effort to face up to the assault, the records proprietor needs to assemble a chain of assignment ciphertexts, which will increase the computing load. Second, as a test, a records consumer needs to decrypt one of the demanding situations ciphertexts, which calls for some of high-priced operations (e.g., pairing). Both sides' computing complexity is always raised on this case, and good-sized community potential is vital for ciphertext transmission. [3] does now no longer well account for the cloud's good sized processing potential. In this work, we are able to offer a singular approach for coping with EDoS assaults that entails much less processing and communication. In a paper by Antonis Machala's [2], a protocol for sharing records was presented, which utilizes a combination of same searchable encryption and (ABE) to enable direct searching of encrypted data. To facilitate important revocation functionality in ABE, the protocol incorporates SGX to host a revocation authority. Bakas and Machala further modified the protocol by proposing a hybrid or blend encryption method that simplifies the process of multiple user record splitting to that of a single user. Specifically, the similar key employed for encrypting data is stored in an SGX enclave, which is itself encrypted using an ABE approach. It, like, makes use of the SGX enclave to address the revocation hassle withinside the context of ABE. In this paper, we use SGX to permit us to limit the download request.

4. Architecture and Security Model

A. System's Architecture

The architectures of our twin get admission to manipulate structures for cloud statistics sharing are proven in Figure 1 depicts the topologies of our twin get admission to manipulate structures for cloud statistics sharing. The structures are made from the subsequent components: The authority is in fee of putting in gadget parameters and registering statistics customers. It additionally handles the cloud name request withinside the preliminary cautioned construction. The statistics proprietor owns the statistics and need to outsource it to the cloud. Data proprietors, in particular, preference to percentage their statistics with men and women who meet precise criteria. They might be disconnected after their statistics has been transferred to the cloud. The statistics consumer needs to retrieve and decode the encrypted statistics that has been shared withinside the cloud. Those who're permitted can down load and decrypt the encrypted material. Cloud garage is a beneficial answer for each statistics proprietors and statistics customers. It particularly saves statistics customers' outsourced statistics and manages statistics customers' down load requests. Enclave procedures the cloud name request (utilized). The following is a creation to workflow. Data proprietors encrypt their statistics the use of get admission to control they pick out and add the encrypted statistics to the cloud. By sending a download request to the cloud, permitted statistics customers can download the shared statistics. When the cloud gets a download request from a permitted statistics consumer (as proven in Fig. 2), it does the subsequent.

a) In our straightforward system, the authority receives an authentication request from the cloud.

b) The cloud replies to the data after getting a response from the authority.

c) In our more sophisticated approach, the cloud requests authentication from the enclave. The cloud then sends a response back to the data user after getting a response from the enclave.

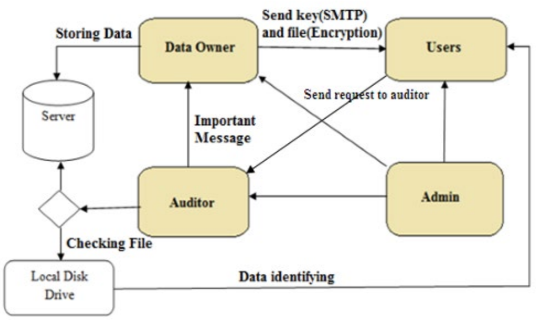


Fig. 2. Architecture diagram

B. Security Assumptions

Each entity's safety assumption is said below. Other entities agree with authority.

The owner of the data is seen as trustworthy since they oversee encrypting it before sending it to the cloud. This is a crucial security precaution that guarantees the data's confidentiality and reduces any potential unauthorized access. The data owner can maintain control over their data and prevent unauthorized access by encrypting the data before re-distribute it to the cloud. • On the other side, a data user can be acting maliciously if they try to download a shared document that they are not allowed to view. They could also launch Edo's (Economic Denial of Sustainability) assaults, which can seriously damage the infrastructure of the cloud service provider. The availability of cloud services is frequently disrupted in these assaults with the intention of causing significant financial and reputational damage. Therefore, it is essential to put in place the proper security measures to stop such attacks and guarantee the system's general security.

5. Goals of Design and Security Requirements

The design objectives of our proposed systems are based on the safety assumptions of each entity mentioned above. In our execution, we can use the SGX SDK cryptography library and upload the statistics-oblivious characteristic to make it safe towards aspect channel attacks

- Data change this is anonymous. The statistics proprietor's identification must now no longer be made public. The cloud can't decide the actual identification of the file's proprietor for a freshly uploaded file.
- Data sharing confidentiality. Data dispatched to the cloud must be invisible to each the cloud and unauthorized statistics consumers.
- Request for nameless download. A download request issued via way of means of a fact's consumer must be nameless withinside the experience that the cloud can't decide who dispatched the request. Control over download requests. To save you malevolent facts customers from launching EDoS attacks, shared facts withinside the cloud can handiest be downloaded via way of means of folks who are accepted.
- Data get right of entry to manipulate for shared resources. Only folks who are accepted can decode the shared facts. Our systems' safety wishes are as follows, primarily based totally on the safety assumptions and layout dreams defined above.
- Protection towards honest however suspicious clouds: Our proposed systems aim to achieve the following design goals to ensure security: The objectives of our proposed systems include:
  a) Preventing the cloud from identifying the originator of a recently uploaded file;
  b) Preventing the cloud from accessing the unencrypted contents of any stored encrypted data;
  c) Ensuring the cloud cannot trace the source of any download request. Furthermore, to safeguard against malevolent data users: i) shared files cannot be downloaded by unauthorized data users; ii) if an illegitimate data user does manage to obtain a shared file, they will be unable to decipher it. A facts consumer is taken into consideration unauthorized if his or her characteristic set does now no longer observe the get right of entry to policy.

A. Use Case Diagram

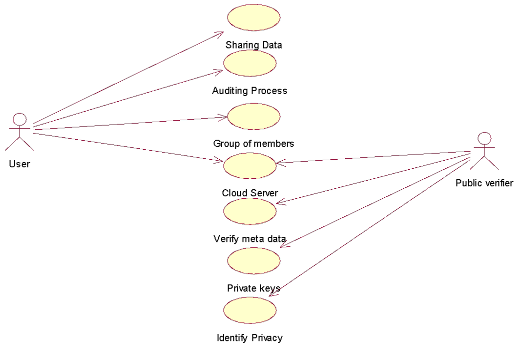


Fig. 3. Use case diagram

The many actors and their interactions with the system are depicted in the use case diagram. The system in this instance is a cloud-based platform for data exchange and storage with dual access control. The data owner, data user, cloud service provider, and access control authority are the actors in this diagram.

The cloud-based platform allows the data owner to upload data and define the access control rules for that data. The data user has the ability to seek access to the data, but access cannot be allowed until the access control authority has given its consent. The data must be stored and managed by the cloud service provider, but access to the data requires sufficient authorization from the access control authority.

B. Flow Chart

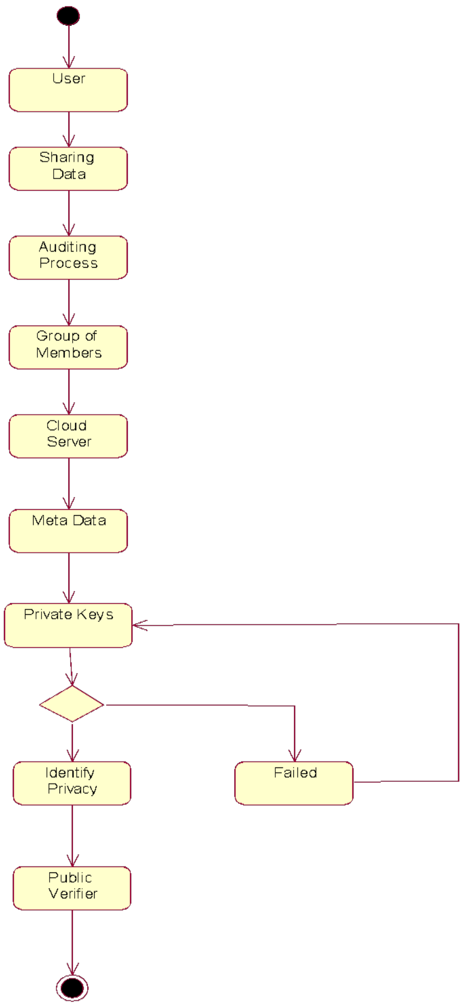
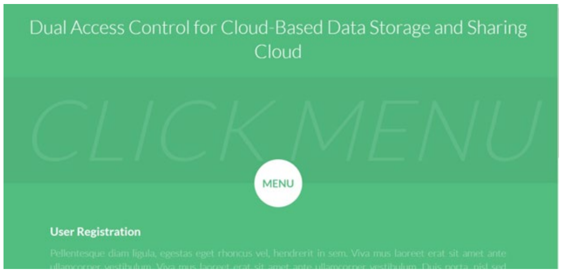


Fig. 4. Flow chart

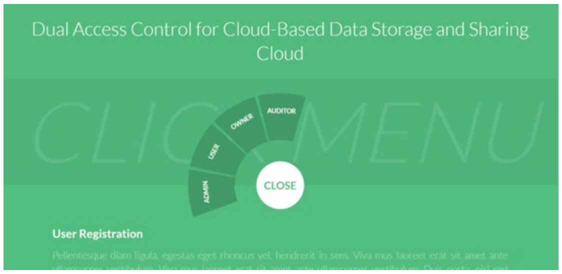
The project's flowchart for "Dual Access Control for Cloud-Based Data Storage and Sharing" illustrates the many procedures that must be taken. The user transmits the data to the cloud at the beginning of the flowchart. The cloud then requests that the authority confirm the user's identity and access rights. Upon getting a reply from the authority, the cloud decides whether or not the user is permitted access to the data. The cloud delivers the user's encrypted data if they are authorized to receive it. The user then uses their private key to decode the data. The flowchart also shows how to terminate a user's access, including procedures for the cloud to delete the user's data and the authorization to terminate the user's access rights.

6. Result


Dual Access Control for Cloud-Based Data Storage and Sharing Cloud

Pellentesque diam ligula, egestas eget rhoncus vel, hendrerit in sem. Viva mus laoreet erat sit amet ante

Fig. 5. Home page


Dual Access Control for Cloud-Based Data Storage and Sharing Cloud

Pellentesque diam ligula, egestas eget rhoncus vel, hendrerit in sem. Viva mus laoreet erat sit amet ante

Fig. 6. Menu page

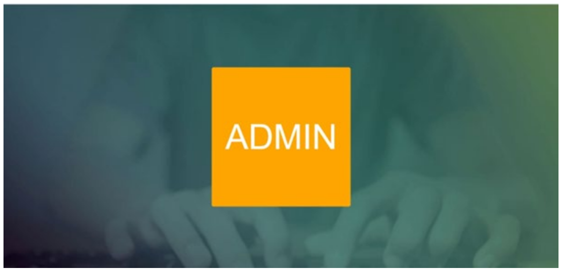


Fig. 7. Admin page

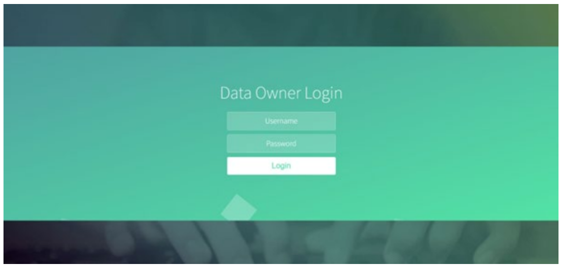


Fig. 8. Data owner page

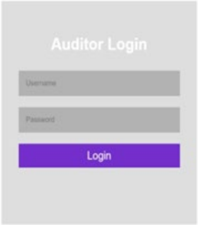


Fig. 9. Auditor page

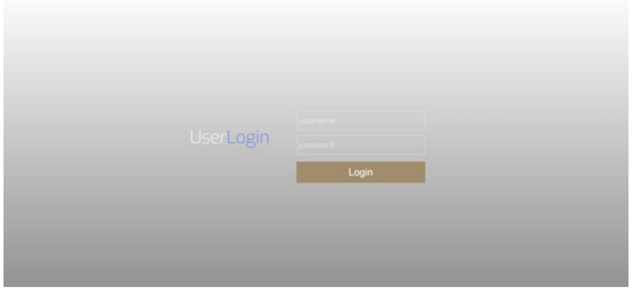


Fig. 10. User login page

7. Conclusion

This study presents a safe and collision-free proxy re-encryption rule and non-traceable and faulter OCLT-ORAM protocol. These protocols enable group data sharing in a cloud storage system. The advised method, that is primarily based totally on key exchange, can correctly produce the customers' convention key, which may be used to protect the safety of shared facts and save you malevolent customers from colluding with different customers. Furthermore, the proxy re-encryption method guarantees the safety of shared institution facts withinside the cloud in addition to get entry to control. Pointer tuples are used to enforce fault-tolerant and tamper-resistant features. The enough safety evidence means that our protocol is steady. The experimental evaluation consequences are probably considered as validation of our protocol's performance, making it a long way greater persuasive.

References

[1] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key exposure resistance," Information Forensics and Security, IEEE Transactions on, vol. 10, no. 6, pp. 1167-1179, 2015.

[2] R. S. Bali and N. Kumar, "Secure clustering for efficient data dissemination in vehicular cyber physical systems," in Future Generation Computer Systems, vol. 57, no. 4, 2016, pp. 476-492.

[3] S. Zarandioon, D. D. Yao, and V. Ganapathy, "K2c: Cryptographic cloud storage with lazy revocation and anonymous access," International Conference on Security and Privacy in Communication Systems, 2011, Springer, pp. 59–76.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in 2010 Proceedings of the IEEE Infocom, IEEE, 2010, pp. 1-9.

[5] M. Ali, R. Dhamotharan, E. Khan, S. Khan, A. Vasilakos, K. Li, and A. Zomaya, "Sedasc: Secure data sharing in clouds," IEEE Systems Journal, vol. 11, no. 2, 2017.

[6] The RFC 1321 document titled "The MD5 Message-Digest Algorithm" describes the MD5 hashing algorithm. MD5 (Message Digest Algorithm 5) is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value.

[7] B. Wang, B. Li, and H. Li, "Certificateless Public Auditing for Data Integrity in the Cloud," IEEE Conference on Communications and Network Security (CNS'13), 2013.

[8] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions on Computers, February 2013.

[9] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE INFOCOM conference, 2013.

[10] X. Sun, J. Yan, L. Zhang, and S. Yu, "Secure and Efficient Dual Access Control in Cloud Computing," Journal of Information Security, 2019.

[11] L. Wang, J. Li, and X. Li, "Dual Key Attribute-Based Encryption with Outsourced Revocation in Cloud Computing," Journal of Network and Computer Applications in 2017.

[12] S. J. E. Adomi, M.A. Omoregbe, and A.S. Iyamu, "A Review of Access Control Mechanisms for Cloud Computing," International Journal of Advanced Computer Science and Applications, 2019.

[13] Li, H. Wang, and X. Sun, "A Secure and Efficient Dual Server Public Key Encryption Scheme for Cloud Storage," Journal Security and Communication Networks, 2016.

[14] S. Wu, X. Sun, Y. Xiang, and C. Wang, "A Lightweight and Efficient Dual Server Public-Key Encryption Scheme for Secure Data Sharing in Cloud Computing."