Nano World Journal

https://doi.org/10.17756/nwj.2023-s4-086

Research Article

Open Access

Cost-effective Data Compression for Unified Access Control in Encrypted Cloud Storage

Harsh Agarwal*, Natta Vignasai, Soorarapu Pavan Kartheek Chary, Baduguna Swapna and Mohammad Manzoor

Department of Information Technology, Vardhaman College of Engineering, Hyderabad, Telangana, India

***Correspondence to:**
Harsh Agarwal
Department of Information Technology,
Vardhaman College of Engineering,
Hyderabad, Telangana, India.
E-mail: harshsinghal1703@icloud.com

Received: September 19, 2023
Accepted: December 04, 2023
Published: December 08, 2023

Citation: Agarwal H, Vignasai N, Chary SPV, Swapna B, Manzoor M. 2023. Cost-effective Data Compression for Unified Access Control in Encrypted Cloud Storage. *NanoWorld J* 9(S4): S509-S513.

Published by United Scientific Group

Abstract

Cloud computing is the trending technology, where multiple users are sharing the data files over the cloud continuously. However, security in cloud environment is the biggest task, where malicious attackers are stealing the data by introducing the attacks. So, the various conventional security protocols were introduced in the cloud environment, which are failed provide the maximum-security standards. Therefore, this work is focused on implementation of Fully Outsourced Protocol (FOP) for providing the higher security standards. Initially, data owners generated the message data, which might be audio, video, data, or textual file. But most of the cases, data contain higher (huge) size, which needs to be optimized. So, data compression applied on the original data, which reduces the memory size of original data. Then, compressed data is applied to the FOP, where Ciphertext-Policy Attribute-based Encryption (CP-ABE) encryption is performed to secure the data. Specifically, Economic Denial of Sustainability (EDOS) attacks occurred in cloud environment, which steals the data from cloud service providers (CSP), data owners, and data users. So, CSP controls the entire environment by introducing FOP with CP-ABE protocol. Here, the attribute authorities are responsible for generating the public key, security key for data owners and data users. Finally, data users receive the secured data. The simulations showed that, the FOP-CP-ABE resulted higher security standards good compression ratios.

Keywords

Cloud computing, Economic denial of sustainability attacks, Cloud service providers, Fully outsourced protocol, Ciphertext-policy attribute-based encryption

Introduction

Important information must be electronically communicated across users inside firms in the paperless workplace of today. Information that has to be shared is kept in one place on a common server, often in the cloud. From there, any authorized user may view the data. Data must be encrypted before sharing since cloud servers are often held by other parties [1]. Only people who are permitted to access the information should be able to access it, which is another security need. The information may be effectively encrypted and decrypted using symmetric encryption methods like AES. Securely distributing the content key for symmetric encryption over a public network is the major difficult requirement [2]. As these methods encrypt data using the public key of the decryptor and decrypt data using the descriptor's private key, they are often used to communicate the secret keys of data files encrypted using symmetric encryption. One-to-one encryption and one-to-many encryption are two types of asymmetric key cryptographic encryption algorithms [3]. This raises a security problem for the owners of the data. Server-dominated access control methods like password- and certificate-based authentication are used by many storage systems. They put a lot of faith in the CSP to safeguard their private information. Any document may

be seen by cloud service providers and their staff, regardless of the access restrictions set by data owners. Furthermore, since there is no structure in place for the accurate measurement of resource utilization. We can have both granular access control and robust secrecy using CP-ABE [4]. The fact that only data owners have access to this access control, however, proves to be inadequate. The cloud must let everyone to download in order to maintain availability if the CSP cannot verify users prior to downloading, as is the case with many current CP-ABE cloud storage systems [5]. The storage system is therefore susceptible to resource-exhaustion assaults. If cloud-side access control is impossible, anyone including hostile attacker must be allowed to download freely, yet only a select few users may decode. Attacks that use all the server's resources are possible. Resource usage will rise when hostile users perform Denial of Services/Disturbed Denial of Services (DoS/DDoS) attacks against cloud storage [6]. The higher consumption brought on by such assaults must be covered by payers (in a pay-as-you-go basis), which is a significant and unjustifiable financial burden. Furthermore, even when files are encrypted, illegal downloads may compromise security by making offline analysis more convenient and disclosing data such as file length. Responsibility for Resource Consumption Users pay the CSP for storage services under the pay-as-you-go approach. Resource utilization determines the price [7]. We employ the challenge-response CP-ABE encryption/decryption game for our cloud-side access control. The data owner first creates some random challenge plaintexts and the accompanying ciphertext before uploading an encrypted file. The ciphertext and the particular file have the same access policy. The cloud server requests that an incoming data user decipher some randomly chosen challenge ciphertext. To avoid EDOS attacks and have granular access control and resource consumption accountability, we provide a universal approach to secure encrypted cloud storage. This is the first type of work to assert that encrypted cloud storage without adequate cloud-side access control would result in EDOS assaults and offers a workable fix. The novel contribution of this work is that the implementation of FOP based CP-ABE security protocol.

A cost-effective data compression-based unified access control for encrypted cloud storage, infused with nanotechnology, exemplifies the convergence of advanced data management and nanoscale innovations. The system leverages nanosized components to enhance the efficiency of data compression algorithms, allowing for streamlined storage in encrypted cloud environments. Nano-enhanced data compression-based unified access control system for encrypted cloud storage represents a forward-thinking approach, ensuring cost efficiency, robust security, and optimized performance in handling sensitive data within cloud environments.

Literature

The CSP (including Google, Amazon, and Microsoft Azure) are modelled in several current ABE-based systems as passive or just partially honest adversaries [8]. However, such a description is limited and leaves out several potential real-world assaults, such excessive resource utilization. In actuality, major IT companies like Google, Amazon, and Microsoft often provide cloud services [9]. They must maintain their good name and assure their clients of the security of their cloud storage services. The CSP dares not cheat if any effort to depart from the protocol is expected to be discovered with a likelihood (for example, p = 0.001) [10]. Because being caught not only violates the service agreements, but also exposes the company to public attention and damages its brand. The CSP must avoid from assaulting since the cheating may be seen in the aftermath. Many safe systems have used the covert security concept [11]. Be aware that the semi-honest paradigm differs from the covert security concept. Between "malicious" and "trusted," the semi-honest approach is a popular one among proxies and CSPs. It simulates a party that monitors all data but never runs the incorrect application. This party is modelled differently by the covert model, which lies in among "malicious" and "semi-honest." [12] It won't run the incorrect application unless there is a way to catch it lying. In other cases, the party may potentially compromise the data if there is no detection in the system. It is hence more useful for public cloud storage. The CSP is not shielded from many additional assaults by the access control system that uses encryption [13]. The CSP cannot halt those illegal users since it does not manage access control. DDoS is one attack that results from this restriction. The DDoS assaults have been shown to use a large amount of CPU, memory, I/O, and network resources [14]. Public clouds are susceptible to assaults and the limitations of the cloud-side static resource distribution paradigm are examined in [15], along with the possibility of EDOS assaults, which are similar to DDoS attacks in a cloud environment and the Fraudulent Resource Consumption attack in [16]. The goal of these assaults is to drain clients of public cloud services of their money.

Existing research [17] makes an effort to reduce EDOS assaults. The authors suggested a mitigation method that involves determining if a request originates from a cloud user or a bot. The authors also suggested an attribute-based method to recognize rogue clients. They do not completely protect the attack at the algorithmic and protocol levels because they perceive the underlying application as a black box. Concerns about the need of accounting for resource use in the public cloud are raised in various previous studies. The writers in the literature [4] explored the major problems and obstacles to achieving accountability in cloud computing. The authors looked at the accounting and accountability practices that are currently used in content distribution systems in the literature. The authors suggested a methodical technique for verifiable resource accounting in cloud computing in the literature [18]. The accounting strategy, nevertheless, calls for modifications to the system architecture and needs users to be verified anonymously, which is not supported by earlier systems. Create protocols that are resistant to a hidden attacker by modelling CSPs as such as partially outsource protocol (POP) [19]. For POP, there are several builds and variations. Because it is difficult to implement all the features in these systems and because it is essential, we should create a novel variation of the POP to address these difficulties. Some variations provide extra security and privacy guarantees on top of the features.

Experimentation

Proposed scheme

Computing in the cloud, in which several users continually share data files with one another, is a cutting-edge technology that is now in demand. In spite of this, ensuring data safety in a cloud environment remains one of the most difficult challenges, as malevolent hackers continue to find new ways to steal data. As a result, several traditional security methods have been implemented in the cloud environment, all of which have failed to achieve the highest possible level of security. Figure 1 shows the block diagram of cloud side access based controlling environment. As a result, the emphasis of this effort is placed on the deployment of the FOP, in order to provide better levels of security. The message data, which might take the form of an audio, video, data, or textual file, was first created by the data owners. However, in the vast majority of instances, the data have a greater size, which necessitates optimization. Therefore, data compression is performed to the initial data, which results in a reduction in the amount of memory required to store the initial data. After that, the FOP receives the data with its compression applied, and then CP-ABE encryption is carried out in order to protect the data. In particular, EDOS attacks have taken place in cloud environments, which have resulted in the theft of data from CSPs, data owners, and data consumers. Therefore, CSP have complete control over the environment with the implementation of FOP and CP-ABE protocol. In this case, it is the responsibility of the attribute authority to generate the public key as well as the security key for the data owners and data consumers. In the end, consumers of the data obtain the protected data. The simulations demonstrated that the FOP-CP-ABE led to better compression ratios while maintaining a higher level of security criteria. To perform EDOS assaults, a rogue attacker may download hundreds of files, which would considerably deplete the cloud resource. The cost is borne by the cloud service subscriber. Additionally, without providing data owners with any transparency, the CSP acts as both the accountant and the payer of resource usage fees. In the actual world, public cloud storage should allay these worries. In this paper, we provide a method for resource responsibility and EDOS protection for encrypted cloud storages. It adheres to CP-ABE's access policy and employs FOP schemes in a black-box fashion. The proposed scheme used to maintain the three controlling environments.

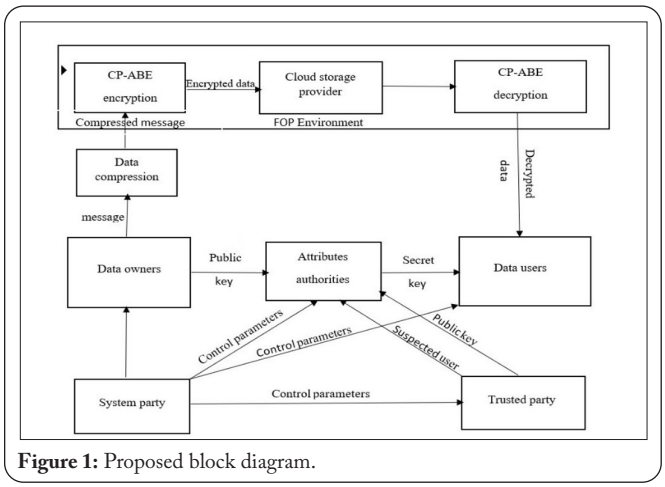

Figure 1: Proposed block diagram.

- Control-1: Data owners authorises the specific (authorized) data users to decrypt the files. Here, trusted party authenticates the attribute authorise, which shares the secret key and public key to data users for decryption of data.
- Control-2: Data owners sent data to CSP, where security protocols maintained effectively and sends the compressed data to data users.
- Control-3: Attribute authorities-controlled system party verifies each file uploaded into CSP, which also verifies each file downloaded at data users. This mechanism alerts the EDOS attack occurs and blocks the malicious users.

Data owners

Data owners upload files, set access controls using CP-ABE, encrypt data, and then provide encrypted data to a third party using secret key data for user authentication. The author acknowledges that major businesses may not defraud clients by claiming that they have used a certain number of resources, but to guard against this possibility the author has given customers the opportunity to confirm resource usage. This feature allows the data owner to ask the cloud for information on his data use or download.

Data compression

Information security in a cloud setting is the most critical factor nowadays as cloud computing has emerged as a vital component of IT. Numerous individuals may utilize the cloud services and facilities depending on their ability. Cloud computing is used for secure data storage, but data security remains the top priority. For example, confidentiality, data accessibility, and data integrity are important factors for cloud storage. Clients are given the option by cloud service providers to store their data offsite and retrieve it whenever necessary. This capability makes it essential to protect or cover information from unauthorized access, hackers, or other types of tampering and malicious behaviour. It is a low-cost method of storing important data and doesn't need hardware or software to save data. Excellent job experience is provided; however, security is the primary factor. In this study, security solutions for cloud data protection have been developed. These strategies use file splitting, compression, and steganography algorithms to increase security while overcoming the drawbacks of traditional data protection algorithms. The client may quickly use the desktop application we designed and transfer the information in an efficient and safe manner thanks to these strategies, which are used for excellent outcomes in data security.

FOP with CP-ABE

In this part, we provide a protocol based on the signature algorithm that is fully outsourced since it does not need an external PKI for resource accounting or challenge generation/updating (FOP). Furthermore, we provide the bloom filter for data owners to save their challenge plaintexts in order to

improve efficiency and, jointly, minimize storage space. This bloom filter may be kept on a cloud server locally or remotely. We refer to the plan as a POP since the data owner must conduct the challenge update procedure on demand or on a regular basis; it cannot be outsourced to the cloud. We vary from POP primarily in two ways:

- The challenges are issued by the cloud rather than the data owners.
- The data owners provide a couple of signatures, public keys for each file, which authorized users use to sign a confirmation to verify the resource use.

The following is a description of the FOP's primary process:

- Securely upload: To upload the secure data in cloud environment.
- FOP-challenge generation: Unlike POP, challenges in FOP with CP-ABE are created by the CSP. Both in advance and on demand generating options are available.
- FOP-challenge response: This process is conducted by the cloud and data owners.
- FOP-resource management: The data owner and the cloud collaborate to accomplish this process.

CSP

This is a cloud server that stores user data, verifies users, and gives data owners information on resource use. We use the CP-ABE algorithm for key creation, data encryption, and data decryption.

Attribute authorities

Users may store data on the cloud and retrieve it whenever they want at a minimal cost. Due to the lack of data owner control over data storage, any data stored in the cloud will be at risk for security. Numerous data security algorithms have been developed to offer data security, with CP-ABE being the most well-known. Any user with access control may request a file from the cloud, download it, and then open it if the user has the necessary permissions in his attributes; otherwise, the file won't be opened. With the help of this technique, access control and data security may be achieved, however CP-ABE has the disadvantage of initially allowing users to download files with or without permission and then allowing them to decrypt them if they have permission. Downloading a file before it has been decrypted may result in EDOS attack. In this scenario, malicious users unable download files (they will download them anyway to cause trouble and charge consumers) and utilize cloud resources, with charges levied against the users as a result. So, FOP based CP-ABE protocol is introduced.

Data users

This user of data asks the cloud to download a file, and the cloud then requests verification from the user by inputting confidential information collected from the data owner. All data owners provide their private information to their consumers.

Results and Discussion

This section gives the detailed analysis of proposed simulation results. Further, the performance of proposed method is compared with other security protocols. Table 1 shows the performance of various compression methods. Here, the original audio file contains 6713 KB of memory, original video file contains 65213 KB of memory, and original data file contains 1873 KB of memory. So, the table 1 shows that the proposed data compression resulted in superior compression ratio as compared to redundant compressor [11], file compressor [13], and system compressor [15] for all audio, video, and data files. Table 2 shows the EDOS attacks-based security performance of various methods. Here, attack detection accuracy (%), malicious user detection accuracy (%), attack prevention accuracy (%) metrics are computed and compared. Further, table 2 shows that the proposed FOP protocol resulted in higher security standards compared to AES [16], ABE [8], and POP [19].

Table 1: Performance of data compression method.

Method	Audio file (KB)	Video file (KB)	Data file (KB)
Redundant compressor [11]	5673	54,733	1304
File compressor [13]	4755	41,363	937
System compressor [15]	3856	30,586	637
Proposed data compression	1800	16,395	204

Table 2: DDOS attack based security performance.

Method	Attack detection accuracy (%)	Malicious user detection accuracy (%)	Attack prevention accuracy (%)
AES [16]	91.056	90.614	92.516
ABE [8]	92.969	90.661	93.905
POP [19]	93.636	92.308	95.456
Proposed FOP	94.927	93.352	95.640

Conclusion

This article is focused on implementation of FOP based CP-ABE protocol. The FOP implementation is the main focus of this effort in order to provide stronger security requirements. The message data, which might be an audio, video, data, or text file, was first created by the data owners. The majority of the time, however, data is larger than necessary and must be optimized. Data compression is therefore applied to the original data, reducing the original data's memory footprint. Then, compressed data is applied to the FOP, where it is encrypted using CP-ABE. EDOS assaults, which steal data from CSPs, data owners, and data consumers, have specifically been seen in cloud environments. As a result, CSPs provide FOP with CP-ABE protocol to govern the whole environment. In this case, the public key and security key for data owners and data users are generated by the attribute authorities. The protected data is then sent to data consumers. The simulations demonstrated that the FOP-CP-ABE produced better compression ratios and greater security requirements. This work can be extended with higher security protocols for better security.

Acknowledgements

None.

Conflict of Interest

None.

References

1. Bouchaala M, Ghazel C, Saidane LA. 2021. Trak-cpabe: a novel traceable, revocable and accountable ciphertext-policy attribute-based encryption scheme in cloud computing. *J Inf Security Appl* 61: 102914. https://doi.org/10.1016/j.jisa.2021.102914
2. Huang K. 2021. Accountable and revocable large universe decentralized multi-authority attribute-based encryption for cloud-aided IoT. *IEEE Access* 9: 123786-123804. https://doi.org/10.1109/ACCESS.2021.3110824
3. Lai J, Guo F, Susilo W, Huang X, Jiang P, et al. 2021. Data access control in cloud computing: flexible and receiver extendable. *IEEE Trans Services Comput* 15(5): 2658-2670. https://doi.org/10.1109/TSC.2021.3057197
4. Ramesh D, Mishra R, Trivedi MC. 2021. PCS-ABE (t, n): a secure threshold multi authority CP-ABE scheme based efficient access control systems for cloud environment. *J Ambient Intell Hum Comput* 12(10): 9303-9322. https://doi.org/10.1007/s12652-020-02643-2
5. He P, Xue K, Yang J, Xia Q, Liu J, et al. 2021. FASE: fine-grained accountable and space-efficient access control for multimedia content with in-network caching. *IEEE Trans Netw Service Manage* 18(4): 4462-4475. https://doi.org/10.1109/TNSM.2021.3096428
6. Razaque A, Shaldanbayeva N, Alotaibi B, Alotaibi M, Murat A, et al. 2022. Big data handling approach for unauthorized cloud computing access. *Electronics* 11(1): 137. https://doi.org/10.3390/electronics11010137
7. Houssein R, Younis YA. 2021. Deploying risk access models in a cloud environment: Possibilities and challenges. In IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA, Tripoli, Libya.
8. Zheng T, Luo Y, Zhou T, Cai Z. 2022. Towards differential access control and privacy-preserving for secure media data sharing in the cloud. *Comput Security* 113: 102553. https://doi.org/10.1016/j.cose.2021.102553
9. Ezhilarasi TP, Sudheer Kumar N, Latchoumi TP, Balayesu N. 2021. A Secure Data Sharing Using IDSS CP-ABE in Cloud Storage. In Arockiarajan A, Duraiselvam M, Raju R (eds) Advances in Industrial Automation and Smart Manufacturing. Lecture Notes in Mechanical Engineering. Springer, Singapore, pp 1073-1085.
10. Xie M, Ruan Y, Hong H, Shao J. 2021. A CP-ABE scheme based on multi-authority in hybrid clouds for mobile devices. *Future Gener Comput Syst* 121: 114-122. https://doi.org/10.1016/j.future.2021.03.021
11. Ma J, Wang M, Xiong J, Hu Y. 2021. CP-ABE-based secure and verifiable data deletion in cloud. *Security Commun Netw* 2021: 8855341. https://doi.org/10.1155/2021/8855341
12. Yang Y, Sun J, Liu Z, Qiao Y. 2022. Practical revocable and multi-authority CP-ABE scheme from RLWE for cloud computing. *J Inf Security Appl* 65: 103108. https://doi.org/10.1016/j.jisa.2022.103108
13. Cheng R, Wu K, Su Y, Li W, Cui W, et al. 2021. An efficient ECC-based CP-ABE scheme for power IoT. *Processes* 9(7): 1176. https://doi.org/10.3390/pr9071176
14. Zhao C, Xu L, Li J, Fang H, Zhang Y. 2022. Toward secure and privacy-preserving cloud data sharing: online/offline multiauthority CP-ABE with hidden policy. *IEEE Syst J* 16(3): 4804-4815. https://doi.org/10.1109/JSYST.2022.3169601
15. Zhang W, Zhang Z, Xiong H, Qin Z. 2022. PHAS-HEKR-CP-ABE: partially policy-hidden CP-ABE with highly efficient key revocation in cloud data sharing system. *J Ambient Intell Hum Comput* 13: 613-627. https://doi.org/10.1007/s12652-021-02922-6
16. Singamaneni KK, Naidu PS. 2022. An efficient quantum hash-based CP-ABE framework on cloud storage data. *Int J Adv Intell Paradigms* 22(3-4): 336-347. https://doi.org/10.1504/IJAIP.2022.124317
17. Sowjanya K, Dasgupta M, Ray S. 2021. A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems. *J Syst Archit* 117: 102108. https://doi.org/10.1016/j.sysarc.2021.102108
18. Sethi K, Pradhan A, Bera P. 2021. PMTER-ABE: a practical multi-authority CP-ABE with traceability, revocation and outsourcing decryption for secure access control in cloud systems. *Cluster Comput* 24: 1525-1550. https://doi.org/10.1007/s10586-020-03202-2
19. Sharma P, Jindal R, Borah MD. 2022. Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. *J Supercomput* 78: 7700-7728. https://doi.org/10.1007/s11227-021-04179-4