IJCS International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012

https://www.ijcsjournal.com/ Volume 10, Issue 2, No 7, 2022. ISSN: 2348-6600
Reference ID: IJCS-455 PAGE NO: 3086-3090

CONTENT BASED DATA TRANSFER IN CLOUD COMPUTING

Mathivanan V
Lecturer, UTAS-Ibra, Oman.

Ramakrishnan R
Lecturer, Yanbu University, Saudi Arabia.

Mohamed Osman Alkaram
Lecturer, UTAS-Ibra, Oman.

Ramesh Palanisamy
Lecturer, UTAS-Ibra, Oman
palanisamy@ict.edu.om

Abstract

The primary goal of this work is to build a secure and efficient protocol that ensures tight security for owner content while also supporting secure data transportation from one Cloud Service Provider to another in an untrusted cloud environment. To address the issues raised, this paper introduced the Content Based Policy (CBP) technique, which is highly resilient and efficient for secure/credential metric data. This CBP technique lowers critical complications while providing tight content security at a cheap communication cost. Here, the data holder can upload a significant amount of content to the cloud, complete with content names and descriptions. A trustworthy user can directly retrieve data with content from this location.

Keywords: Cloud Service Provider, Content Based Policy, Retrieve Data, Security.

Introduction

Various research organizations and corporations have studied the phrase Cloud Computing and defined it in various ways and dimensions. According to [1,] cloud computing is a collection of the fewest number of elements that are present in the majority of the given list of virtualization, cost-usage service model, and reliability. The emphasis is on virtualization technology, which distinguishes it because it can function independently of any other technology. National Institute of Standards and Technology (NIST) from United States of America in its 16th version stated, "Clouds are a huge set of straightforwardly serviceable and reachable virtualized properties which incorporates hardware, software, and infrastructure based features". These sources can be lazily re-configured to govern an unpredictable pack (size) while also functioning as the best alternative for resource exploitation. This class of assets is typically used to implement a price-based model that Infrastructure service providers can use.

The Cloud Research team eventually strives to gain a thorough grasp of the fundamental components of cloud computing from a technology standpoint for clients or users. For example, the preliminary description in [3] envisions a cloud technique. It is a mirror bonding of critical cloud tools such as statistical hubs and hardware tools with their respective locations.

Literature Survey:

This study [2] provides a novel public-key cryptosystem with fixed-size cipher-texts, allowing for proficient delegations of decryption privileges for any collection of cipher text. The ability to aggregate any set of secret keys and transform them into a compact single key distinguishes the proposed approach. The author of this study [3] describes the construction of a simple content privacy model in which data is encrypted using the Advanced Encryption Standard (AES) before being stored in a cloud server, ensuring content confidentiality and increased security from external threats.

The authors of this research [4] discuss Cipher Cloud, which secures user data on public cloud infrastructures. To ensure that data transported from a client to a cloud server or vice versa is completely protected and confidential, Cipher Cloud employs a two-step encryption procedure. In this study [5,] the authors suggest a simple data protection architecture that uses Advanced Encryption Standard (AES) before storing data in the cloud, ensuring data confidentiality and security. The author updated his privacy strategy in this study [6], which includes four methodologies: Resilient Role-based Access Control Mechanism (RACM), Partial Homomorphic Cryptography (PHC), Metadata Generation (MG), and Sound Steganography (SS). These approaches are primarily concerned with the efficiency of third-party auditing services, data backup and recovery processes, and owner/user content.

Content Based Policy (Cbp) Approach

CBP (Content Based Policy Algorithm) is a public key cryptographic system designed for one-to-many communication [10]. A public key is described in CBP, along with a combination of the various properties and their data linkage [11]. The message details and a set of public key attributes were used in the encryption process. In accordance with their access rights, trusted users are assigned an access key to access the mechanism. The secret key reflects the content attribute access structure that fulfills the users access mechanism [12].

Three different datasets have been chosen to evaluate the proposed method: documents, images, and videos. During the installation and testing phases, the data sets are considered with a steady rise in size, which aids in achieving a very trustworthy outcome. In this system, a JAVA-based Secure Storage & Retrieval system is utilized to retrieve data from a centralized server. These datasets aid in the system's evaluation process, demonstrating its efficiency, simplicity, and integrity for cloud-based applications.

Communication Cost

The proposed method in this part addresses the mathematical model as an equation (1). It calculates the transmission cost (%) depending on the length of the content and the sized index of the attribute content. It considers the average performance of encryption and decryption of a specific content collection. The cost of communication is c(|q|+|n|) bits.

$$MC = c(|q|+|n|)---(1)$$

Where c represents the size of the content, |q| represents the length of an element, and |n| represents the length of an index. In depth. This method describes and analyzes a dataset that includes documents, photos, and video. Table 1 summarizes the analysis results in terms of communication cost (%), encryption time (in sec), and decryption time (sec). The tabular result also compares to known algorithms like as DES [7], 3DES [8], BLOWFISH , RC6 , RSA , and ABE [9]. These factors, such as CC, ET, and DT values, are derived both experimentally and conceptually from numerous study articles. Finally, this study claims that the new CBP methodology outperformed previous strategies.

Table 1: Communication cost

Algorithm	Document	Images	Video
	Communication Cost in %		
DES	65.4	48.5	50.2
3DES	59.8	50.6	61.9
BLOWFISH	66.9	83.5	81.4
RC6	70.2	51.2	63.5
RSA	57.5	31.1	41.2
ABE	94.4	95.5	96.4
CBP	99.7	99.2	89.8

Table 1 represents the simulation result of CBP approach along with many existing approaches in tabular format. This approach is evaluated with communication cost, encryption time, and decryption time with different kinds of dataset and sizes.

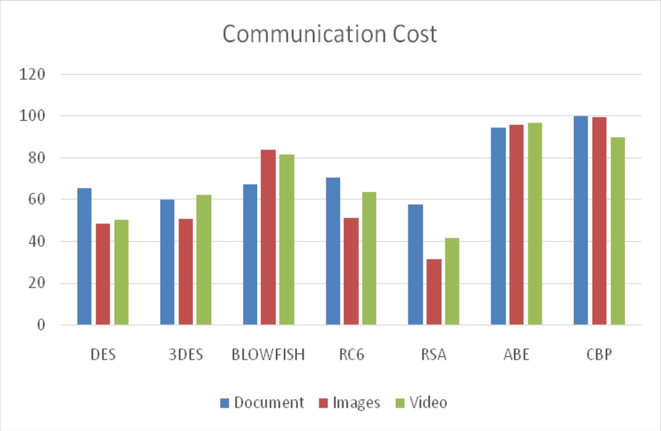

Figure 1: Communication cost (%)

Figure 1 represents graphically the communication cost (%) for all existing methods along with proposed CBP approach for document, images and videos dataset.

Content Based Policy Approach is being implemented and the result are being tabulated and presented in graphical format as well. The evaluation is done based on various parameters such as Communication Cost. Datasets of various categories such as Documents, Images and Videos are taken into account with various sizes. CBP approach is evaluated with regards other existing models like AES, RSA, ABE, DES, TRIPLEDES, and BLOWFISH. This research work also addresses differences against with existing methods and their overall results is presented clearly. After evaluation of simulated result, we claim that CBP is best protocol to implement even in un-trusted cloud environment.

Conclusion:

In this thesis, this research work initially elaborates cloud environment, types of cloud, cloud infrastructures and cloud service details. Next, this research work identified the most critical problem from several existing methods of cloud environments which have been gathered by reviewing various research articles and applications. To design a solution for the congregated problem, this work proposes Content Based Policy (CBP) technique which is highly robust and efficient for secure and credential metric data.

References:

[1]. Xinyi Huang, Joseph K. Liu, Shaohua Tang, Yang Xiang, Kaitai Liang, Li Xu, Jianying Zhou, (2014), “Cost-Effective Authentic and Anonymous Data Sharing with Forward Security” IEEE Transactions on Computers, Vol. 64 , Issue 4, Pages 971 – 983.

[2]. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, (2014), “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage” IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, Pages 468 – 477.

[3]. SanjoliSingla& Jasmeet Singh, (2013), “Implementing Cloud Data Security by Encryption using Rijndael Algorithm”, Global Journal of Computer Science and Technology Cloud and Distributed, Vol. 13 Issue 4, Pages 18-22.

[4]. Manpreet Kaur, and Rajbir Singh, (2013), “Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing”, International Journal of Computer Applications, Vol. 70, No.18, Pages 16-21.

[5]. AbhaSachdev and MohitBhansali, (2013), “Enhancing Cloud Computing Security using AES Algorithm”, International Journal of Computer Applications, Vol. 67, No.9, Pages19-23.

[6]. Sarfraz Nawaz Brohi, MervatAdibBamiah, SuriayatiChuprat, Jamalul-lail and Ab Manan, (2014), “Design and Implementation of A Privacy Preserved Off-Premises Cloud Storage”, Journal of Computer Science, Vol. 10 No. 02, Pages 210-223.

[7]. Sonal Guleria1, and Dr. Sonia Vatta, (2013), “To Enhance Multimedia Security in Cloud Computing Environment using Crossbreed Algorithm” International Journal of Application or Innovation in Engineering & Management (IJATEM), Vol. 2, Issue 6, Pages 562-568.

[8]. Abdul, D. S., Elminaam, H. M. A. K., &Hadhoud, M. M, (2009), “Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA, Vol. 8, Pages 58-64.

[9]. Madnani , B. R., &Sreedevi N., (2013), “Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 3, Pages 523-530.

[10]. Ramakrishnan, R., &Mathivanan, V., “A Criticism of Contemporary Cloud Computing Productions and Encounters”,International Journal of Computer Engineering & Technology (IJCET), ISSN NO 09766375 /67 Volume 06, Issue 07, pp. 41-50, 2015(Impact factor 8.99).

[11]. Ramakrishnan, R., &Mathivanan, V., “Content Based Security Policy in Cloud Environment”, International Journal of Applied Engineering Research (IJAER), , ISSN: 0973 4562, Volume 10, No. 14, pp. 34658 – 34663, 2015 (Impact factor 0.130)
.

[12]. Ramakrishnan, R., &Mathivanan, V., “Privacy Proof of Data Transportability from one Cloud to another Cloud Service Provider”, International Journal of Control Theory and Applications, ISSN No: 0974 5572, Volume 08, Issue 02, 2015 pp. 38.

[13]. MATHIVANAN, PALANISAMY, R. A. M. E. S. H., VIMAL, SENTHIL, & RAFI. (22AD). Cloud Computing Distinctiveness In The Real-Time Environment. International Journal of Scientific Research & Engineering Trends, 8(3). https://doi.org/ ISSN (Online): 2395-566X .

[14]. Stephen, V. K., V, M., Kaliyamoorthy, K., Ullah, M. T., & Palanisamy, R. (2022). Challenges of implementing industry 4.0 in financial sector of Oman. International Journal of Economics and Management Studies, 9(1), 35–38. https://doi.org/10.14445/23939125/ijems-v9i1p106.