International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Comparative Study of Encryption Algorithms for Cloud Computing

Madhura Mahajan[1], S. C. Dharmadhikari[2]
[1]PG Scholar, Department Of Information Technology, Pune Institute of Computer Technology, Pune, India
[2]Professor, Department Of Information Technology, Pune Institute of Computer Technology, Pune, India

***Abstract*: Cloud computing is extensively used but it's not completely trustworthy. It can be in terms of protecting or securing the confidential data from malicious attacks as well as from cloud providers. Also once the data is deployed on cloud, the user has no control over it. So rather than deploying the original text file the user encrypts the file and then uploads on the cloud. When this file needs to be shared with other it can be done using CP-ABE algorithm (Cipher text policy attribute based encryption). This gives the central access to the owner. Yet this doesn't sufficiently secure from EDoS attacks. Moreover, the decryption schemes also vary from one cloud provider to other. The payer of cloud service bears the expense. Besides, the cloud provider serves both as the payee of resource consumption fee, lacking the transparency to data owners. Hence, this dissertation work proposes methodology to secure or protect encrypted cloud storage from EDos attacks.**

***Keywords*: Cipher text policy attribute based encryption, access control, accounting.**

1. Introduction

Cloud computing has been around for very nearly two decades and 69 percent of organizations everywhere throughout the world are as of now utilizing cloud innovation, and 18 percent have intended to execute distributed computing arrangements in their setups. Distributed computing works on a comparable guideline as online email customers, enabling clients to get to the majority of the highlights and records of the framework without keeping the heft of that framework all alone PCs. Truth be told, a great many people as of now utilize an assortment of distributed computing administrations without acknowledging it'Gmail, Google Drive, TurboTax, and even Facebook and Instagram are all cloud-based applications. For these administrations, clients are sending their own information to a cloud-facilitated server that stores the data for later access. What's more, as helpful as these applications are for individual utilize, they're considerably more profitable for organizations that should have the capacity to get to a lot of information over a safe, online system association. When you're on the cloud, simple access to your organization's information will spare time and cash in task new businesses[1]. Furthermore, for the individuals who are concerned that they'll wind up paying for highlights that they neither need nor need, most distributed computing administrations are pay-as-you-go. This implies on the off chance that you don't exploit what the cloud brings to the table, at that point at any rate you won't need to drop cash on it. The compensation as-you-go framework likewise applies to the information storage room expected to benefit your partners and customers, which implies that you'll get precisely as much space as you require, and not be charged for any space that you don't. Taken together, these variables result in lower costs and higher returns. Information proprietors who store records on cloud servers still need to control the entrance without anyone else hands and keep the information secret against the cloud supplier and noxious clients. Encryption isn't Sufficient: To include the classification ensure, information proprietors can scramble the records and set an entrance arrangement with the goal that just qualified clients can decode the archive. With Ciphertext-Policy Attribute-based Encryption (CP-ABE), we can have both fine-grained get to control and solid privacy.

Nonetheless, this entrance control is accessible for information proprietors, which ends up being lacking. On the off chance that the cloud supplier can't validate clients before downloading, as in many existing CP-ABE distributed storage frameworks, the cloud needs to permit everybody to download to guarantee accessibility. This makes the capacity framework defenseless against the asset fatigue assaults. In the event that we settle this issue by having information proprietors confirm the downloaders previously enabling them to download, we lose the adaptability of access control from CP-ABE. Here records the two issues ought to be tended to in our work: Problem I (Resource-Exhaustion Attack): If the cloud can't do cloud-side access control, it needs to permit anybody, including vindictive aggressors, to unreservedly download, albeit just a few clients can unscramble. The server is defenseless against asset depletion assaults. At the point when noxious clients dispatch the DoS/DDoS assaults to the distributed storage, the asset utilization will increment. Payers (in pay-as-you-go display) need to pay for the expanded utilization contributed by those assaults, or, in other words and nonsensical budgetary weight. The assault has been presented as Economic Denial of Sustainability (EDoS), which implies payers are monetarily assaulted in the long run. Also, even documents are encoded, unapproved downloads can decrease security by bringing

comfort to disconnected examination and spilling data like record length or refresh recurrence. Issue II (Resource Consumption Accountability): In the compensation as-you-go demonstrate, clients pay cash to the cloud supplier for capacity administrations. The expense is chosen by asset use. Notwithstanding, CP-ABE based plans for distributed storage get to control does not make online affirmations to the information proprietor before downloads. It is required for the cloud specialist organization to demonstrate to the payers about the genuine asset use. Something else, the cloud supplier can charge more without being found.

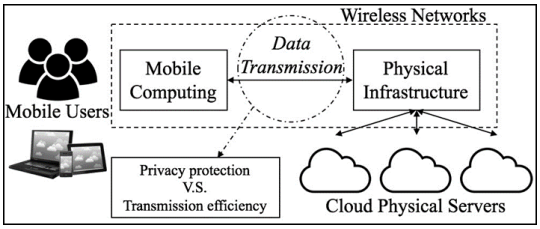

Fig. 1. Architecture of cloud computing illustrating the balance between privacy protection and transmission efficiency

There are numerous developments and variations for CP-ABE. We don't plan another variation of CP-ABE to determine the main test, as it is difficult to accomplish every one of the functionalities in these frameworks and furthermore it's a bit much. Other than the functionalities, a few variations give extra security and protection ensure. For instance, the literary works conceals the entrance strategy. On the off chance that the cloud-side access control makes the cloud supplier knowing the entrance approach, it isn't viewed as secure and good. It requires the cloud-side access control to be zero-learning for discretionary CP-ABE plans. Approach: utilize CP-ABE in a linguistic and discovery way and guarantee the development not spilling strategy and properties. To ensure the distributed storage viably against the asset fatigue assault, the cloud-side access control should be effective and lightweight, generally if the cloud server spends, for instance 20ms, executing the cloud-side access control, it will end up being a computational asset depletion assaults, which can be utilized by noxious aggressors for DDoS and EDoS. The execution overhead being little additionally benefits the information clients who download the documents from the distributed storage, making the calculation not agreeable to asset restricted gadgets.

2. Literature survey

A. Combining data owner-side and cloud-side access control for encrypted cloud storage [1]

People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy-sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, cipher text-policy attribute-based encryption (CP-ABE) can be utilized to conduct fine-grained and owner-centric access control. However, this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provides the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch economic denial of sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage.A solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of the CP-ABE.

B. Privacy-preserving verifiable set operation in big data for cloud-assisted mobile crowd sourcing [2]

In smart city, all kinds of users' data are stored in electronic devices to make everything intelligent. A smart phone is the most widely used electronic device and it is the pivot of all smart systems. However, current smart phones are not competent to manage users' sensitive data, and they are facing the privacy leakage caused by data over-collection. Data over-collection, which means smart phones apps collect users' data more than its original function while within the permission scope, is rapidly becoming one of the most serious potential security hazards in smart city. The current state of data over-collection and study some most frequent data over-collected cases. A mobile-cloud framework, which is an active approach to eradicate the data over collection. By putting all users' data into a cloud, the security of users' data can be greatly improved. Extensive experiments and the experimental results have demonstrated the effectiveness of the approach.

C. Digital signature security using cryptography for industrial applications

For ranked search in encrypted cloud data, order preserving encryption (OPE) is an efficient tool to encrypt relevance scores of the inverted index. When using deterministic OPE, the ciphertexts will reveal the distribution of relevance scores. Therefore, a probabilistic OPE,called one-to-many OPE, for applications of searchable encryption, which can flatten the distribution of the plaintexts. A differential attack on one-to-many OPE by exploiting the differences of the ordered ciphertexts. The experimental results show that the cloud server can get a good estimate of the distribution of relevance scores by a differential attack. Furthermore, when having some background information on the outstheced documents, the cloud server can accurately infer the encrypted keywords using the estimated distributions.

Table 1
Comparative study

No.	Title	Author	Publication & Year	Technique/ Algorithm Used	Strength	Weakness
1	Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage	Kaiping Xue , Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong	IEEE Trans-actions on Information Forensics and Security, 2018	Partially Outsourced Protocol, Fully Outsourced Protocol	CP-ABE schemes in arbitrary access policy by perfor-mance and security analysis.	The cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners.
2	Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowd sourcing	Gaoqiang Zhuo, Qi Jia, Linke Guo, Ming Li , and Pan Li	IEEE Internet of Things Journal	Big Data, Mobile Crowd-sourcing, Verifiable computation	Extensive performance analysis and experiment-based on real cloud system have shown both the feasibility and efficiency of our proposed scheme	Limited computation and storage resources, cloud-assisted approaches may serve as a promising way to tackle big data analysis issue.
3	Cloud EFS: Efficient and Secure File System for Cloud Storage Clemens	Zeidler Depa, Muhammad Rizwan Asghar	IEEE Transactions on Cloud Computing 2016	Efficient Storage of data on cloud and out sourcing	CloudEFS provides improved privacy by hiding not only content but also metadata such as data size, file count, file structure and file history.	Large data it becomes difficult to access and update data, and to ensure data integrity and data provenance without decrypting all the data.
4	Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds	Dan Gonzale,Jeremy Kaplan, Evan Saltzman, Zev Winkelman, Dulani Woods	IEEE Transactions on Cloud Computing,2015	Cloud computing, cyber security, advanced persistent threats, security metrics, virtual machine (VM) isolation	Cloud-Trust is used to assess the security level of four multi-tenant IaaS cloud architectures equipped with alternative cloud security controls	A wide range of security controls and best practices are essential
5	Concrete Attribute-Based Encryption Scheme with Verifiable Outsourced Decryption	Charan, K Dinesh Kumar, D Arun Kumar Reddy	IJETT – Volume 12 Number 9	Attribute-based encryption, outsourced decryption, verifiability.	A significant reduction on computing resources imposed on users	Selectively data can be shared only at a coarse-grained level.
6	A New Bloom Filter Structure for Identifying True Positiveness of a Bloom Filter	Ju Hyoung Mun, Jungwon Lee, and Hyesook Lim	IEEE, 2017	Bloom filter techniques, Petit-BF (P-BF)	The P-BF method can achieve the same performance using a considerably smaller amount of memory.	Every element included in the complement set of the given set should be programmed into the C-BF.
7	Digital Signature Security Using Cryptography for Industrial Applications	Dr.(Mrs.) Ananthi Sheshasaayee, Mrs. B.Anandapriya	Inter-national Conference on Innovative Mechanisms for Industry Applications,ICIMIA 2017	Digital signature, Hash functions and RSA.	Digital signature confirmation conspire gives secure correspondence between two clients.	Imprints empower acknowledgment and check of the believability of paper records,
8	Privacy Preserving in TPA for Secure Cloud by using Encryption Technique	Roshni Singh, Ataussamad, Dr. Shiva Prakash	ICIIECS 2017	Privacy Preserving, Third Party Authority, Public Auditing	Achieve the privacy preserving public for auditing	Doubt in its integrity due to the existence of software/ hardware error along with human error too.
9	Identity-Based Remote Data Integrity Checking with perfect Data Privacy Preserving for Cloud Storage	Yong Yu, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min	IEEE Transactions on Information forensics and Security, Vol. 12, No. 4, April 2017	Cloud storage, data integrity, privacy preserving, identity-based cryptography.	Secure against the malicious server in the generic group model and achieves zero knowledge privacy against a verifier	Proving to a verifier that it is actually storing a data owner's data.
10	Privacy protection for preventing data over-collection in smart city	Y. Li, W. Dai, Z. Ming, and M. Qiu	IEEE Transactions on Computers, 65:1339–1350, 2016	Access Control Service, database, Encryption	the operations of encryption and decryption were achieved by cloud encryption/decryption service that saves computation resource	Data over-collection in smart phone becomes the most severe potential privacy hazard in smart city

D. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage [9]

Currently, privacy leakage has become a great concern when a web-based application is applied. The threats deriving from communications are generally caused by implementing lower-level security protocols. However, using a higher-level privacy protection approach is often restricted by the efficiency requirements, since an enhanced security level needs a longer execution time than the approach offering a lower-level privacy protection. The proposed approach is called Dynamic Multi-Channel Communications (DMC2) model, which is designed to dynamically determine the transport layer protocols in terms of the timing constraints. Consider four contemporary deployed protocol types the optional channels and the method can produce optimal solutions to maximizing the privacy level. The experimental evaluations have examined the performance of DMC2, which demonstrates its privacy protection capability and the adaptability.

3. Algorithm

The procedure of POP is described in detail as follows: [1] Encrypt and Upload (POP-EU): This operation is implemented by an individual data owner independently, which can be divided into the following four steps.

POP-EU-1: The data owner uses hybrid encryption to encrypt the message. The data owner randomly selects a symmetric key k ←$ {0, 1}λ and uses the key to encrypt the message M. Then the data owner encrypts that symmetric key k with CP-ABE under A:

c0 ← AEAD.Enc (k, "message" _ M) ,

c1 ←ABE.Enc (mpk, k,A) ,

c2 ←SIG.Sign (skowner, c1).

POP-EU-2: The data owner randomly generates N challenge plaintexts from the message space. They should be different with each other.[1]

{ chal1, chal2 , . . . , chaln }, chali←$ {0, 1}L.

The data owner generates the hashes of these challenges:

hashi = H(chali), ∀i ∈ [1, N],

where H(•) is a collision-resistant hash function.

For each challenge plaintext chali , the data owner uses k to encrypt it with a fixed prefix "challenge".

The prefix makes these challenges different from messages, which prevents the cloud from deceiving the users into decrypting messages instead of challenges. Here the encryption is also under the same hybrid encryption structure:

enchali = AEAD.Enc(k, "challenge"||chali).

c3 = {hashi }i∈[N],

c4 = {chali }i∈[N] .

POP-EU-3: The data owner creates a bloom filter to store the challenge plaintexts. We denote m as the size of the bloom filter.

bf ← BF.Setup (m, λ) ,

∀i ∈ [N], bf ← BF.Insert (bf, chali).

And then the data owner encrypts the bloom filter:

c5 = ABAE.Enc (k, bf) ,

where k is the data owner's secret key. Note that to avoid the cloud provider understanding the structure of the bloom filter, the data owner should use its own keyed hash functions in the element insertion and test. The data owner keeps the version number of the bloom filter to thwart rollback attacks is an assumption

POP-EU-4: The following tuple is uploaded to the cloud:

ct = (c0, c1, c2, c3, c4, c5).

4. Conclusion

Thus the conclusion of the above survey can be stated as a consolidated the cloud-side and information proprietor side access control in distributed storage, or, in other words DDoS/EDoS attacks gives resource consumption accounting. Our framework bolsters self-assertive CP-ABE developments. The development is secure against malignant information for clients and covert cloud providers. The security prerequisite of the cloud supplier to secretive foes, or, in other words down to earth and loosened up thought than that with semi-legit enemies. To make utilization of the incognito security, we utilize bloom filter and probabilistic check in the resource consumption accounting to decrease the overhead. Execution demonstrates that the overhead of development is little over existing frameworks.

References

[1] Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong, "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage", IEEE Transactions On Information Forensics And Security, Vol. 13, No. 8, August 2018.

[2] Gaoqiang Zhuo, Qi Jia, Linke Guo, Ming Li , and Pan Li, "Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowd sourcing", , IEEE Internet of Things Journal

[3] Zeidler Depa, Muhammad Rizwan Asghar, "CloudEFS: Efficient and Secure File System for Cloud Storage Clemens",IEEE 2016.

[4] Dan Gonzales, Member, IEEE, Jeremy Kaplan, Evan Saltzman, Zev Winkelman, Dulani Woods, "Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds", IEEE Transactions on Cloud Computing.

[5] Charan, K Dinesh Kumar, D Arun Kumar Reddy,"Concrete Attribute-Based Encryption Scheme with Verifiable Outsourced Decryption", (IJETT) – Volume 12 Number 9.

[6] Ju Hyoung Mun, Jungwon Lee, and Hyesook Lim, " A New Bloom Filter Structure for Identifying True Positiveness of a Bloom Filter", 2017 IEEE

[7] Ananthi Sheshasaayee, Mrs. B.Anandapriya, "Digital Signature Security Using Cryptography for Industrial Applications", International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2017).

[8] Roshni Singh, Ataussamad,Dr. Shiva Prakash, " Privacy Preserving in TPA for Secure Cloud by using Encryption Technique", ICIIECS 2017.

[9] Yong Yu, Man Ho Au, Member, IEEE, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min, "Identity-Based Remote Data Integrity Checking with perfect Data Privacy Preserving for Cloud Storage", IEEE Transactions on Information forensics and Security, Vol. 12, No. 4, April 2017.

[10] Y. Li, W. Dai, Z. Ming, and M. Qiu., "Privacy protection for preventing data over-collection in smart city," IEEE Transactions on Computers, 65:1339–1350, 2016.