The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 695 – 702

Enhanced Symmetric Convergent Encryption for Secured Data Deduplication in Cloud

Dr. G. Uma
Assistant Professor- PG & Research Department of Computer Science
Srimad Andavan Arts and Science College(Autonomous)-Trichy.
venkataraman_uma@yahoo.co.in

Abstract: Cloud storage is a virtual setting that includes an amazing amount of processing power. The resources are in a state where they can serve users. Cloud data centres are the locations where all of this computing is maintained. In order to produce high-performance computing, the data centre houses a sizable number of powerful computers and servers connected to one another. The physical computer resources housed in the cloud data centre are accessible to the user via virtualization. To provide a convergent encryption method that will enhance data security while reducing deduplication's impact on security, encryption, and decryption times. Convergent encryption is used to prevent duplicating data, but the key used to encrypt data for the first time is kept up to date and distributed to all users who have same or closely related content of data to upload to the cloud storage. In an open cloud environment, it's crucial to distribute the key to all users. When using cloud storage services, users encountered numerous issues.

Key words: Deduplication, Convergent Encryption, Cloud Environment, Key.

Introduction

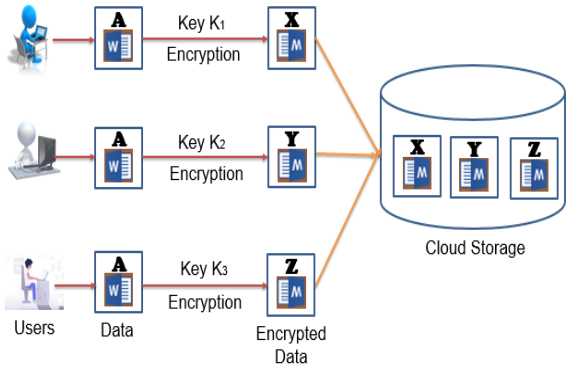
A virtual environment with a staggering amount of processing power is cloud storage. The resources are in a state where they can serve users. Cloud data centres are the locations where all of this computing is maintained. A sizable number of powerful computers and servers connected to one another in the data centre produce high-performance computing [1]. The physical computing resources in the cloud data centre are accessible to the user via virtualization [2]. Data storage in cloud storage is the main goal of using the cloud [3]. . In the upcoming years, maintaining and storing data will be essential duties. Because, according to an IDC research, data output has surged recently, and by 2020, The amount of data we can store will be 40 quadrillion gigabytes [4]. It appears that the only choice for maintaining and storing this enormous amount of data in the future is the cloud to support the cloud, properly maintain data, and prevent storing duplicate copies of data there. Data deduplication is a well-known method used in the cloud to prevent duplicate copies of data [5]. The data being submitted to a website is verified by data deduplication.

Deduplication and Convergent Encryption

Data deduplication eliminates the duplicate storing of data in the cloud.
It enables the cloud to store just one copy of the data in the cloud.

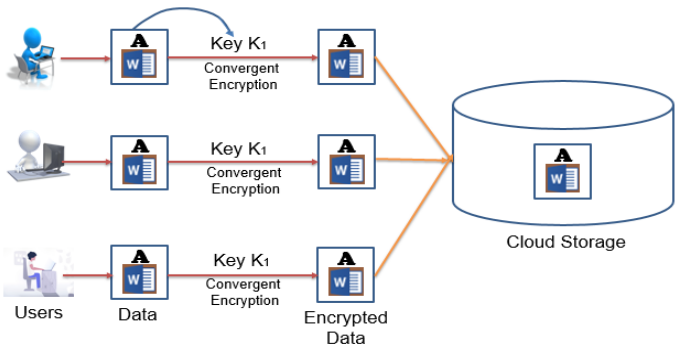
The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 695 – 702
Due to the rise of the cloud, users are ready to move their data there, however there are concerns over the security of data kept there. The perfect cloud challenge to address is data security [6]. Many research solutions exist [7][8][9] that use cryptographic approaches to address the security of data in the cloud. Data are encrypted using a cryptographic technology, Afterward, they are saved on the cloud using a secret key.

User data is encrypted [10] before being transferred to the cloud to guard against insider threats. Each user uses a secret key to encrypt the data, which makes data deduplication difficult because a separate secret key generates a distinct ciphertext for the same copy of the data. Therefore, classical encryption creates many copies of the data in various encrypted forms.



Data storage using Traditional Encryption Approach

The same data is encrypted by each user using a different key based on their preferences, which results in different encrypted data that is stored independently in cloud storage. To solve this problem and enable efficient deduplication in cloud storage, CE [11] is utilised. The hash key used by Convergent encryption, also known as the convergent encryption key, is produced from user data. . Data is encrypted using convergent encryption technique and convergent encryption key. Convergent encryption prevents duplicating data in cloud storage, as seen in Figure 5. 2. The plaintext data that is being uploaded to the cloud is used to generate the convergent encryption key, This is subsequently applied to ciphertext to encrypt plaintext. The same plaintext data will generate a convergent encryption key if another person has access to it. The identical ciphertext is generated using the same key and data; however, only one copy of the ciphertext is now kept in cloud.



Data Storage using CE Approach

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 695 – 702
Deduplication is supported by convergent encryption to reduce redundant data. It offers the cloud system greater benefits to properly maintain cloud storage. In addition to all of this, existing convergent encryption methods are more susceptible to dictionary and brute-force assaults [12]. because the convergent encryption key, also known as a hash key, is produced without the usage of a secret key.

Therefore, this key is simple for hackers to decrypt. The convergent encryption key may occasionally be generated using a key. In this situation, the user must create and keep the key. if it is lost, the data is vulnerable for hacking. The key to being saved on the user's side will also grow in number as more data is generated at the same time. The maintenance of keys and metadata details places an increased workload on users [13]. The preceding chapter suggested a convergent encryption key generation algorithm to solve the issues mentioned above. For safe data storage, this chapter suggests the JAUM Cipher, an asymmetric convergent encryption method. The suggested Enhanced Symmetric Convergent Encryption Algorithm uses the convergent encryption key generated from the users' data to produce the same encrypted data. In the structure outlined in chapter 3, the proposed convergent encryption JAUM cypher is offered as a Convergent Encryption as a Service (CEaaS).

Vulnerabilities on Convergent Encryption

The only effective strategy to keep a unique copy of data in the cloud is data deduplication. There are numerous deduplication methods that researchers have suggested. Convergent encryption is the primary function of deduplication; however it is susceptible to brute force and dictionary attacks [12]. A poison assault, also known as a duplicate fake attack or an erasure attack, in which a malevolent opponent replaces the original with the corrupted file, is a possibility with convergent encryption. Because of this, trustworthy users lose their files and forced to download fraudulent versions [15]. Another problem with convergent encryption is the confirmation of a file attack, in which an attacker can conclusively establish whether a target has a certain file by scrambling an unencrypted or plain-text version and then directly comparing the result with files the target is in possession of. [16]. This attack creates the appearance of a difficulty for a user who is storing non-unique information, i. e., data that is either publicly available or that the adversary already has [17]. It is impossible to perform deduplication using conventional cryptographic approaches.

Instead, convergent encryption uses the user data to generate a key, that is used to encrypt the user data [18].

Methodology

The cloud offers a modern platform for maintaining user data. Users should guarantee the security of the data stored in the cloud. The encrypted data is kept on the cloud via a technique called cryptography. Convergent encryption, however, is utilised to maintain safe cloud storage with unique data copies in order to maintain efficient data storage. We can produce the same encrypted data for the same original data copy thanks to convergent

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 695 – 702
encryption. The suggested method creates a convergent key using information from the users. Users create the encrypted data by encrypting it with the convergent key. After the data has been encrypted, a tag is created during the deduplication process from the encrypted file, and it is forwarded to the cloud to be checked for duplication. A new link is generated and given to the user if the tag is already present in store. User can upload the data to cloud in any case. The suggested method uses cloud services for encryption and key creation. These services should be used by users to obtain the key and establish their identity before receiving the key and data.

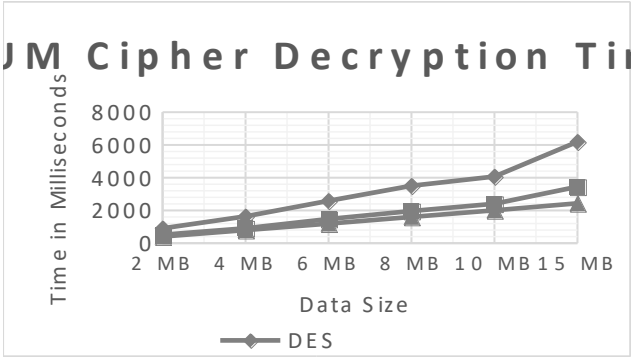
Proposed Convergent Encryption

The data was treated at the bit level by the suggested convergent encryption. The data is encrypted using CEK created by the user with the aid of KTaaS. 128 bits make up the key. Users' data is separated into 128-bit blocks, which are then XORed together using the key. Before the users' data are used to determine the complement of this one. The ciphertext is created by dividing the bits into 8 bits and converting them to ASCII characters after the calculation. This encrypted text has been stored in the cloud.

Comparison of Time for Encryption

Size	**Encryption Techniques**		
	DES	**Blowfish**	**JAUM Cipher**
	(Milliseconds)		
2 MB	948	582	428
4 MB	1679	986	833
6 MB	2627	1522	1238
8 MB	3575	2034	1637
10 MB	4106	2499	2047
15 MB	6288	3502	2468

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 695 – 702



Comparison of Time for Encryption

Results

The suggested research effort, is described in detail in this section along with the simulation setup. An environment for simulation research is developed. The simulation environment for this study effort has already been covered in chapter 3. All of this thesis's suggested research projects use the same setup. A cloud-based application for better symmetric convergent encryption is created with C#. Net and Visual Studio 2012. The application is hosted on the Microsoft Azure platform. In order to provide deduplication services using CE and key generation, the hosted application is configured as a cloud application. Applications for cloud services also use KTaaS coding. The hosted application has provisions for overall research work, which entails creating a token from user data, sending a request for data uploading, receiving a key from KTaaS, creating a convergent key, encrypting data with that key, creating tags, checking tags for deduplication, uploading data to a cloud server, checking the user for ownership proof, and allowing users to download their data from the server. All of these procedures are programmed into the Microsoft Azure Platform application. Only the CEaaS element is the focus of this chapter. The Amazon and Google Cloud Platforms both allow for the creation of the same simulation setup. On the Azure platform, the created cloud application for JAUM Cipher is hosted. The screenshots that follow were also captured from the cloud server's running application.

Security Measure and Comparison

The security level parameter serves as a gauge for convergent encryption power. By employing a security hacking tool called the hack man tool, the offered tactics' security level is evaluated as analyst. Based on the tool for planned and current procedures, the security level is assessed.

Hackman analyst the security level of each technique by using the formulas described as follows.

Considered that, Let M be the size of ciphertext from the cloud storage, I represent the size plaintext recovered by the attack on ciphertext by using Hackman tool.

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 695 – 702
The following formula measures the proposed and existing encryption algorithms' security level,

$$P = M - I$$

Here, P represents the size of data recovered data by Hackman which are not mapped with plaintext text.

Consequently, the formula for finding the security level in percentage is,

$$S = \frac{P}{M} * 100$$

Here, S represents the security of proposed CTs in EOaaS in percentage, and the % of insecurity level is measured by,

$$IS = \frac{I}{M} * 100$$

Here, IS represents the insecurity of each algorithm.

By altering the data produced by the appropriate algorithms, the Hackman tool evaluates how secure each existing and suggested algorithm is.

Research Findings and Interpretations

Effective deduplication makes it possible for the cloud to offer storage in a safe way.

A CE method was suggested in this chapter as a cloud service.

Convergent encryption is susceptible to several attacks, including brute force, dictionary, and attacks like poison, as was stated earlier. The key and algorithm for the suggested method are obtained via the cloud service. Users don't want to keep the algorithm or key in their possession. According to the technique, users should generate the CEK based on a GKCEK that is generated from the cloud. Additionally, users receive encryption through the ECaaS cloud service, and data is secured on the user side, using the CEK. Additionally, users receive encryption through the ECaaS cloud service, and data is secured on the user side, using the CEK. Because erasure attacks are impossible, it protects against attacks like brute force, dictionary, and poison attack. Deduplication begins with the user's data (UDTKNGKCEKCEKEDTG), which is then forwarded to a cloud server to be checked for duplication before a fresh link is created for user. Else, the ED is uploaded to the cloud server while being encrypted. The techniques for the suggested solution ensure that deduplicated data is secure while also providing efficient storage management.

Conclusion

Data duplication is a crucial step in the process of managing cloud storage securely and productively, and convergence encryption is a key component. In order to secure the data in cloud with deduplication, this chapter had suggested an improved symmetric convergent encryption technique called JAUM Cipher. Based on the specified techniques, the suggested method efficiently processes the data. Based on the process outlined in the previous chapter, the key required for encryption is generated. The user encrypts the data, which is then uploaded to the cloud after being checked for duplication there. The cloud server's study of

the proposed encryption algorithms' effectiveness and efficiency. The cloud environment is used to replicate the full study project. The proposed encryption method was created as a cloud application and is hosted on the Windows Azure cloud infrastructure. The proposed method's encryption and decryption times and security level are simulated. The results are obtained, and it is discovered from the findings that the suggested JAUM Cipher has the highest level of security when compared to other encryption approaches while requiring the least amount of time for encryption and decoding.

Advantages

1. Reduce the multiple storage allocation for a data.

2. Ensure the security of data uploaded to the

cloud.

3. Users can receive any data from the cloud

at any time.

References

[1]Arockiam, L, Monikandan, S, &Parthasarathy G 2011 Cloud computing: a surveyInt. J. Internet Comput1pp 26-33.

[2]Uma G, Jayasimman L 2018 Survey on Data Deduplication Techniques used forEfficient Management of Cloud StorageInternational Journal of Scientific Research in Computer Science Applications and Management Studies72018 pp 163-170

[3]Uma G, Jayasimman L 2018 Enhanced Convergent Encryption Key Generation for Secured Data Deduplication in Cloud Storage JPhCS 1142 (1).

[4]David Reinsel, John Gantz and John Rydning 2017Data Age 2025: The Evolution of Data to Life-Critical Don’t Focus on Big Data; Focus on the Data That’s Big,

[5]https://www. seagate. com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017. pdf pp 1-25.

[6]Mark W. Storer, Kevin Greenan, Darrell D. E. Long, Ethan L. Miller2008 Secure Data Deduplication, ACM proceeding of Storagepp1-10.

[7]Arockiam L,Monikandan S 2013 Data security and privacy in cloud storage using hybrid symmetric encryption algorithm International Journal of Advanced Research in Computer and Communication Engineering28pp 3064-3070.

[8]Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou 2014 A Hybrid Cloud Approach for Secure Authorized Deduplication, IEEE Transactions on Parallel and Distributed Systems pp 1-12.

[9]Uma G, 2018 Optimized Data Storage for Cloud Computing Environment, International Journal of Electrical, Electronics & Computer Science Engineering, special issue

[10] Megala D, S. Pothumani, C. Anuradha 2017 Secure and Efficient De-Duplication System in Cloud Computing, International Journal of Pure and Applied Mathematics, 11620 pp 531-535.

[11] ArockiamL, MonikandanS 2014 Efficient cloud storage confidentiality to ensure data security. IEEE International conferernce prod. inComputer Communication and Informaticspp1-5.
[12] Uma G, Jayasimman L 2018 Cloud Storage Optimization using Compression Techniques IJCSE 123-127.
[13] Taek-Young Youn, Ku-Young Chang, Kyung Hyune Rhee, and Sang Uk Shin2 2016 Authorized convergent encryption for client-side deduplicationIT CoNvergencePRActice (INPRA)4 2 pp 9-17
[14] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P. C. Lee, and Wenjing Lou2014 Secure Deduplication with Efficient and Reliable Convergent Key Management IEEE Transactions on Parallel and Distributed Systems256 pp 1615-1625.
[15] MihirBellare, SriramKeelveedhi, Thomas Ristenpart 2013 DupLESS: Server-Aided Encryption for Deduplicated Storage, Proc. of the 22th USENIX Security Symposium (SEC’13)pp 179–194.
[16] Ashish Agarwala, Priyanka Singh and Pradeep K. Atrey 2017 DICE: A Dual Integrity Convergent Encryption Protocol for Client Side Secure Data Deduplication, IEEE International Conference on Systems, Man, and Cybernetics (SMC) pp 2176-2181.
[17] Zooko Wilcox-O'Hearn, 2008 Drew Perttula and Attacks on Convergent Encryption, 2018 https://tahoe-lafs. org/hacktahoelafs/drew_perttula. html, accessed on September 2018.
[18] Convergent encryption, 2018 https://en. wikipedia. org/wiki/Convergent_encryption, accessed on April 2018.