Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

ESCET: Enhanced Symmetric Convergent Encryption Technique To Provide Secured Deduplicated Data In Public Cloud Storage

K. Balaji[1] , Manikandasaran S S[2]

[1]Research Scholar, PG and Research Department of Computer Science, Adaikalamatha College, Vallam, Thanjavur, Tamil Nadu, India. Affiliated to Bharathidasan University, Trichy, TamilNadu ,India.

[2]Asst. Professor, PG and Research Department of Computer Science, Adaikalamatha College, Vallam, Thanjavur, Tamil Nadu, India. Affiliated to Bharathidasan University, Trichy, TamilNadu ,India.

Abstract

The most sophisticated data storage in the current information technology is cloud storage. Cloud storage mainly helps Small and Medium-scale Enterprises (SMEs) to reduce their investments and maintenance of storage servers. Most small companies outsource data to cloud-based storage. User data transmitted to the cloud must be stored in the public cloud environment. The data stored in the cloud storage may combine with the data of other users. This will cause a data security problem in cloud storage. If the confidentiality of cloud data is compromised, this may result in data loss to the industry. Privacy settings ensure Cloud-based storage security. In order to maintain confidentiality, the most common technique used in security is encryption. However, traditional encryption creates many duplicate data in the cloud storage, which may cause cloud storage management issues. Duplicate data occupies unnecessary storage allocation, creating confusion in the cloud storage. To avoid duplicated data and also provide security, convergent encryption is proposed in this paper. Convergent encryption is a technique to avoid duplicate storage in the cloud and maintain the data's confidentiality. Confidentiality is one of the security services to address the data security issues in cloud storage. The proposed work is measured with previous methods based on the encryption and decryption time, and the security level is measured using ABC Hackman Tool.

Keywords : Cloud computing; Cloud Storage; Deduplication; Encryption; Confidentiality, Cryptography.

1.Introduction

Cloud computing provides massively scalable computing resources as a service equipped with Internet technologies. Resources are shared between many consumers, reducing the cost of computer ownership [1][2]. Cloud computing is currently a topic of much discussion in

academic and industrial circles. With virtualization and distributed computing technology, cloud computing integrates computing, storage, networking, and other computing resources and rents users. Such a mode could reduce the cost of enterprise information construction and accelerate the informatization of enterprise. Cloud storage is designed for the virtualized computing environment[3]. Cloud computing delivers cloud storage, which means taking advantage of the cloud service provider's software and hardware resources. The growth of cloud computing is phenomenal across the global IT industry. While cloud computing has many advantages, some businesses still do not accept using it. As a result, the cloud data security issue has not been fully addressed.

Cloud-based storage provides virtual space for bulk data storage. However, the data owners take no control over their data. The cloud provider consumes full control over the user's data. This makes the user's mind think about the data security in the cloud[4]. Data protection in cloud storage is the core security problem. Data protection [5] relates to confidentiality, integrity, authentication, availability and so on. Data confidentiality means that only authorized persons have the right to use the data. Data integrity is information that has neither been altered nor changed. Authentication refers to the user authorization verification process. Finally, data availability refers to ensuring that data is used when needed and that cloud service providers are available when requested. Security is addressed at different levels. Figure 1 represents the

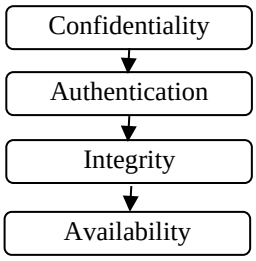

Figure 1 Data Security Layers

order of addressing security in cryptography[6].

The first layer is available, ensuring that the necessary cloud resources or cloud service providers are available when requested. The second layer is authentication, which protects the entry of unauthorized users into the cloud. The third layer is confidentiality, which guarantees that privileged cloud users only have access to data. The final layer is integrity, which prevents unauthorized cloud users from modifying cloud data. Authentication techniques can be used for data protection against external attacks. Confidentiality could be used to protect data from outsiders and internal attacks. If the confidentiality of the data is fully ensured, integrity shall also be ensured. If intruders cannot access data in cloud storage, they cannot be modified or modified by intruders. Although attackers break the authentication mechanism, data in the cloud is always secure when an efficient confidentiality mechanism is used[7].

This article offers efficient cloud storage confidentiality techniques. The well-known confidentiality techniques are encryption techniques. Encryption converts the readable text into an illegible form using an algorithm and a key. Many traditional encryption algorithms are

available in the field of security. However, the point to be noted is that they may provide security to data, but it creates many duplicate data when it is encrypted. Traditional encryption generates different encrypted data according to the key used for encryption. The key used for encryption is based on the user. If any two users have the same content of data, which the key of a different user may encrypt, then the encrypted data for the same content is different[8]. Therefore, the data may be stored in thecloud as different data. Figure 2 shows how traditional encryption stores data in the cloud.

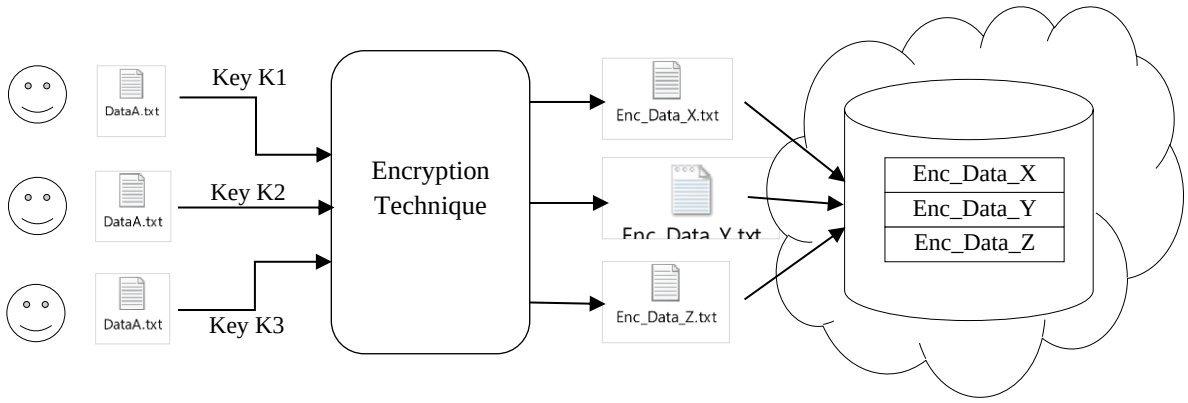

Figure 2 Traditional Encrypted Data Storagein Cloud

The figure shows the traditional storage of encrypted data in the cloud where the same data from different users are encrypted using the same technique with different keys. The result is different encrypted data, and it is stored in the cloud as different data. Hence, it allocates unwanted storage allocation in the cloud. Consequently, it creates storage management headaches. The encrypted data generated for the same data is also the same to handle this situation. To generate the same encrypted data for the same plaintext data is only possible when using the same key at all times. Therefore, each independent user should use a common mechanism to generate the key for the data. This key generation mechanism should generate the same key for the same plaintext data from different users. If all the users have the same key, they can generate the same encrypted data for similar plain text data. Convergent encryption techniques only carry out generating the same key for similar data. The convergent encryption uses the same key for the same plain test data with all the users[9]. Figure 3 shows how convergent encryption stores the data in cloud storage.

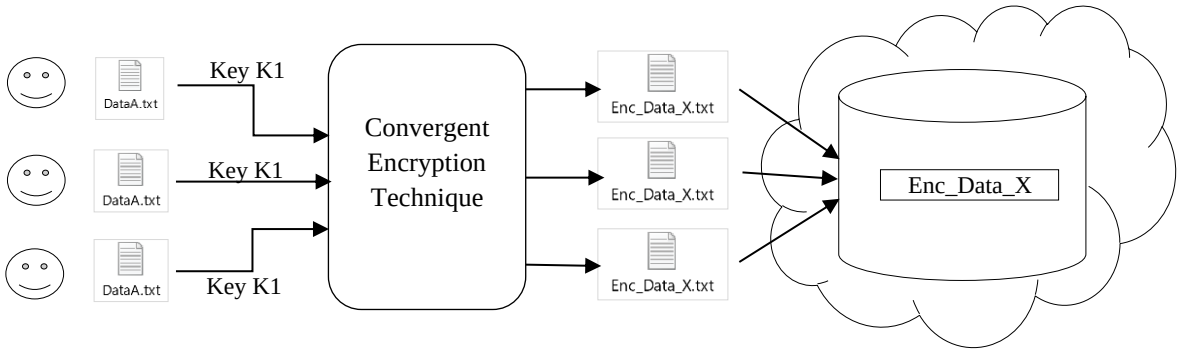

Figure 3 Convergent Encrypted Data Storage in Cloud

Convergent encryption generates the same encrypted data for the same plaintext data supplied from different independent users. This method avoids duplicate data being stored in the cloud. The mechanism of maintaining a single copy of data in cloud storage is called deduplication [10]. The deduplication maintains efficient cloud storage, and it provides security for data in the cloud storage. The research work aims to provide better security with deduplicate data in the cloud. The paper concentrates on proposing an enhanced symmetric convergent encryption technique to provide secured deduplicate data in public cloud storage. This research work is one of the works of the core research work. The core research proposes a secured and deduplicated framework for the public and private cloud. As a part of the core research work, convergent encryption is proposed in this paper. This contribution is a cloud service from the core research framework.

2.Importance of Cloud Data Storage and Security

Cloud storage service is very popular in the business environment. It saves the hardware cost, the cost of the technical personnel needed to manage the database, and saves the cost of licensing the database. In addition, it offers reliable services, and people can access their data 24 x 7 from everywhere where the Internet connection is available. Cloud data storage helps users to outsource their data. Data Outsourcing management is an essential part of cloud storage. As a result of rapid advances in network technology, the cost of transmitting one terabyte of data over long distances has declined considerably over the past decade [11].

Moreover, the total cost of data management is five to ten times the original acquisition cost. This results in organizations outsourcing their data to a cloud storage provider with a nominal rate[12]. This means that the database outsourcing model allows cloud users to use their data better.

Even with the benefits of cloud storage, many people are still concerned. This is probably due to the various safety issues that are still outstanding. Security becomes a severe issue with cloud storage when there are multiple virtual machines (that can access databases via any number of applications). It could be able to access the database unnoticed or trigger alerts. In this type of situation, a malicious individual could potentially obtain relevant data or cause serious damage to the entire database structure, thereby endangering the entire system. This is

the biggest issue with data storage in the cloud. Thus, an effective security model must address this problem in storing data in the cloud. According to the research work, although malicious individuals access the data, they cannot be read or modified[13].

3.Related Work

Ensuring user data security in cloud storage is the major research problem. Cloud storage providers store critical user data, which requires security. Cloud computing has recently achieved success in the information technology field and has dominated the industry for years. However, the cloud is also facing crushing challenges. To ensure the appropriate physical, logical and personal security controls, especially in data storage in the cloud, are more important. In addition, while shifting such volumes of data, data management may not be entirely trustworthy. This section describes research related to security data in cloud storage.

Yoshita Sharma et al. [14] proposed AES, an RSA algorithm that provides multilevel encryption and decryption processes to help secure the data being stored. However, this technique is not easy to crack as an unauthorized user would need the encryption keys and the decryption keys to view or obtain data, which would become difficult to accomplish without a valid key. Nevertheless, multilevel encryption is expected to deliver more safety to cloud storage data than single-level encryption.

Jianting Ning et al. [15] proposed a hybrid system to protect the data, which combines the efficiency of a symmetric-key system with the convenience of a public-key system. In particular, the proposed dual access control systems are in the Key/Data Encapsulation Mechanism (KEM/DEM) setting. The message is encrypted by an efficient symmetric-key encryption scheme, while the inefficient public-key scheme (i.e., the CP-ABE) is used only to encrypt/decrypt a short key value.

Jian Wang et al. [16] proposed that some ciphertext policy attribute-based encryption (CP-ABE) schemes have been applied to cloud data access control to protect data security and privacy. However, two emotional issues, attribute revocation and policy updating, need to be solved in the existing CP-ABE schemes. The proposed fine-grained dynamic multi-authority cloud data access control scheme can solve the two problems.

Soumalya Ghosh et al. [17] proposed methods for Data Encryption and password hashing. This method addressing the security issue in the cloud proposed a salted password hashing technique, a one-way function. So, it is easy to encrypt in one direction using the salted hashing technique, but decryption in the reverse direction is nearly infeasible. It is a fixed-length set of strings that contains a random number and letters in some powerful hashing algorithms special character is also used; the string acts as a “fingerprint” to authenticate the password. If even a bit is changed in the password, the hashed string will be completely different. Hashing the asymmetrically encrypted private key will make it a step ahead in security and overcome security threats.

Adesh Kumari, M. et al. [18] proposed a key agreement framework using smartcard and elliptic curve cryptography (ECC) techniques. The key agreement is achieved between user and cloud. This technique is secure and efficient in terms of computation and communication cost. The proposed protocol may be useful in post-quantum cryptography. However, it is a real-life application for the network system.

Yogita Deepak Sinkar et al. [19] discussed security issues for protecting the privacy of the data. The proposed framework combined two metaheuristic algorithms, the Glowwarm swarm optimization algorithm and the Whale optimization algorithm. This developed GSOA is a glowwarm Swarm whale optimization algorithm. The Cleveland data set is used for the experiment.

Arfatul Mowla Shuvo et al. [20] proposed an approach that is storage efficient and eliminates the issue of data security for distributed cloud-based storage (STaaS) with the use of data compression and cryptography procedures. First, the transferred data to the cloud will be compacted and encoded with compression and Encryption algorithm, and afterwards, the output data will be chunked and stored onto the distributed storage, which will make the transferred data hard to get any access even for the cloud service providers without data owner's permission. Furthermore, if data compression and encryption are executed simultaneously, it requires less processing time and more speed.

Magesh Kumar S et al. [21] proposed a system of cryptographic hash function and data deduplication addressed for getting optimized storage in terms of capacity optimization in a secure manner. The Capacity Optimization using Cryptographic Hash Function and Data Deduplication Cryptographic hash procedures have various data security applications, curiously in computerized marks, Message Authentication Codes (MACs), and different types of justification. This function is used as standard hash capacities to record data in hash tables, fingerprinting, perceive duplicate data or especially recognize reports, and as checksums to distinguish impromptu data debasement. The information security settings, cryptographic hash regards to a great extent called (computerized) fingerprints, checksums, or essentially hash regards, with different properties and purposes.

Tirapathi reddy et al. [22] proposed Advanced Encryption Standard (AES), wherein deduplication is worked out safely. The method invoked privacy and security are duplicated. Deduplication can be done on two sides; one is on the server-side called server-side deduplication, and the other is performed on the client-side, namely client-side deduplication. Server-side deduplication is the one where already stored is deduplicated. Considering that the client-side deduplication is executed while uploading the file or some sort of data, the file would be uploaded if the file on the server does not exist. Client-side deduplication is more powerful than client-side deduplication in most conditions. However, it is equally more important to ensure privacy and one's own is protected. The secured data deduplication to be

implemented to solve duplicate information is removed while maintaining the confidentiality of customer data. This technique approaches its unique structure for encrypting and decrypting sensitive data. This AES algorithm performs on bytes rather than bits. This algorithm uses a key to scramble the data, and the key size used for an AES cipher determines the number of ciphers used to modify the contribution to the last yield, called the plaintext, called the ciphertext, to be interpreted.

Haoran Yuan et al. [23] proposed the re-encryption deduplication storage system. The method proposed a secure data deduplication scheme with efficient re-encryption based on the convergent all-or-nothing transform (CAONT) and randomly sampled bits from the Bloom filter. Due to the intrinsic property of the one-way hash function, this scheme can resist the stub-reserved attack and guarantee the data privacy of data owners' sensitive data. Moreover, instead of re-encrypting the entire package, data owners have only been required to re-encrypt a small part of it through the CAONT, thereby effectively reducing the computation overhead of the system.

4.Methodology

The proposed work is provided as a cloud service; the benefit of this work is to provide a security service using symmetric convergent encryption. This work is one of the proposed works of the research addressing the security and deduplication issue in the public cloud. This proposed work is provisioned from a cloud service is called Enhanced Convergent Encryption as a Service (ECEaaS). ECEaaS is a cloud service provided by the proposed core research work framework. Different clouds and cloud services are designed in the proposed core secured framework. Mainly, security services provided by the ECEaaS is the scope of this work.

Along with ECEaaS, another cloud service is included in the framework for verifying data deduplication called Data DeDuplication as a Service (DDDaaS). The DDDaaS maintains all the details about the data stored in the cloud. It has database details about the file, convergent key, tag, etc. Using the convergent key and the tag, DDDaaS verifies the deduplicated data. Another service named Key Management as a Service (KMaaS) is a key providing service to the encryption techniques in the ECEaaS. The encryption techniques used in the framework are convergent. The key for the encryption is also a convergent encryption key. The key is generated for the user based on their wish with the help of KMaaS. Based on the encryption technique chosen by the user, keys are generated from data uploaded to the cloud.

The framework separates the cloud services, including security, key, deduplication, and storage services. Independent services providers provide all these services. Different independent cloud service providers provide these services. Hence, the storage providers do not know which security techniques and the key to hide the data. Likewise, the key service provider does not know in which cloud the data are stored. This scenario avoids the security risk of the data stored in cloud storage. The framework considers data storage in the public cloud and private cloud. For each cloud data, there is a different convergent encryption technique proposed in ECEaaS. This paper proposed the convergent encryption helps secure and deduplicate the data in the

public cloud. Figure 4 shows the abstract view and component in the proposed core framework of the research. When users want to store data in the public cloud, the ESCET procedure is invoked and encrypts the data; data deduplication also verifies the data for duplicates.

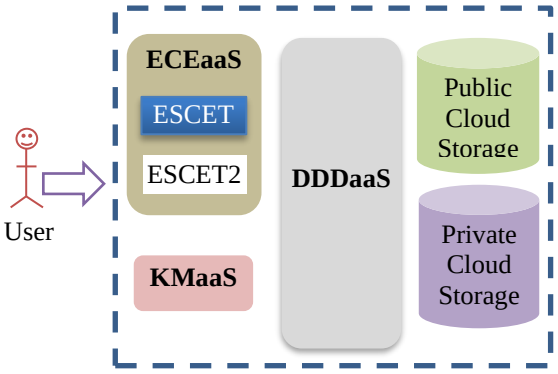

Figure 4 Abstract view of the proposed framework

5.Proposed ESCET Procedure

Cloud computing provides an effective storage setting for storing and retrieving essential data from cloud users. This means that data security plays a vital role for cloud users and providers. The paper uses the confidentiality and deduplication parameters to deal with data security issues. Symmetric encryption is the best choice for cloud data storage because symmetric encryption has the speed and efficiency of computation for high-volume data encryption. In addition to the data security, it also provides a deduplication mechanism to improve data storage management of cloud storage. The proposed ESCET is a symmetric block cipher encryption technique. It uses 160-bit keys for encryption and decryption. The technique runs variable numbers of rounds according to the key. The 160- bit key is divided into five subkeys that are SK1 to SK5.

The SK1 8-bit subkey denotes the number of rounds the encryption or decryption is carryout. The SK2 8-bit subkey is used with PT for finding product value. The SK3 8-bit subkey denotes the number of the circular shift of the decimal PT values. The SK4 128-bit subkey for finding XoR with 128-bit value. The SK5 is an 8-bit subkey used for finding 8-XoR operation. Unlike existing encryption techniques, the number of rounds is not fixed. Instead, rounds are changed based on the SK1 value. This is because the cryptography operations of substitutions and permutations confuse and diffuse the cryptanalyst.

The main key 160-bit is generated from the input data given by the user to upload. Therefore, convergent encryption first generates the key from the data uploaded to the cloud. After generating the key, according to the proposed procedure, it is divided into five subkeys. For example,

Considered the sample 160- bit convergent key:

11000100 00110010 10010010 01000001 11000111 00110100 11000101 11010010 11011110 00100011 00111100 10101011 01101010 00000010 11010000 01101100 01101010 10010100 01011010 01110111

Here,

SK_1→8-bit→11000100

SK_2→8-bit→00110010

SK_3→8-bit→10010010

SK_4→128-bit→ 01000001 11000111 00110100
11000101 11010010 11011110
00100011001111100101010 11
01101010 00000010 11010000
01101100 01101010 10010100
01011010

SK_5→128-bit→01110111

The SK_1 denotes the number of rounds; however, in the 8-bits of SK_1, the first four bits are not considered, and the remaining four bits are considered for denoting the number of rounds.

For example,

SK_1→~~1100~~0100→0100→4, from this key it denotes 4 rounds.

The SK_3 and SK_5 are incremented by value 1 after using the data one time. The SK_4 is a 128-bit key; however, it is equally divided into two 64-bit keys for XoR with 64 bits data of two blocks. When the key is divided according to the methodology, the proposed procedure for ESCET is invoked for encryption. Procedural steps followed when invoking the ESCET is given below.

Procedures involved in the ESCET

1. User submits the plaintext data (PD) and key (K) for encryption
2. ESCET consider 128 bits block bit from the PD for encryption
3. Determine the decimal values in the PD bits.
4. The Key K is divided into five subkeys from SK_1 to SK_5
5. The SK_1 denotes the number of rounds encryption is to be done
6. Encryption begins to find the Product(PDT) of SK_2 and PD, PDT←SK_2 * PD
7. Calculate the square (SQ) for each value in the MT, SQ=square(PDT).
8. Rotate SQ at SK_3 number of times; SK_3 is incremented by 1 for consecutive SQ values. Rotation_SQ (RTN) = $R_{SK2+j}{}^{(SQ)}j = 1,2,\ldots<N$ (R denotes Rotation)
9. Calculate modulus (MD) for RTN by 256, MD=RTN%256.
10. Convert the mod values to binaries; it is equal to 128 bits
11. Divide the 128 bits into 64 bits of two blocks
12. Construct two 8X8 matrices for both 64 bits values
13. Find XoR with two 64 bits keys of SK_4
14. Interchange the odd columns from both 8X8 matrices
15. Find transpose matrix for each 8X8 matrix

16. Read the bits from the matrix and merge two 64 bits into 128 bits
17. Split 128 bits into 8 bits blocks
18. Find XoR for each 8bits with the 8bit key SK_5.
19. Convert the 8 bits values to corresponding into decimal values.
20. Repeat the step from step 6 to 19 at SK_1 times
21. Find the ASCII character code to produce ciphertext (CT).

The ESCET procedure is invoked according to the core framework of the research. The framework initially verifies all the data submitted by the user for the deduplication based on the token generated from the data. If the generated token does not exist in the DDDaaS database, this ESCET procedure is invoked to encrypt the data.

6.Implementation Setup and Results

The proposed research work is coded and developed as a cloud-based service. The developed application is deployed in the MyASP.NET cloud server. The MyASP.NET is a cloud-based platform providing service that enables the users to deploy their application to get a cloud-based experience. The cloud-based application is developed and hosted on the cloud server. The proposed application is developed in C#.NET using visual studio 2012. The hosted cloud application is served as a cloud service consumed by all procedures proposed in the core research work. This paper only concentrates on the implementation and running of the ESCET. It is integrated with one more encryption technique, and both encryptions are provisioned from the cloud service called ECEaaS. ECEaaS is a cloud service comprised of the procedures of the two encryption techniques. Among them, one is ESCET. Figure 5 shows the abstract diagrammatical representation of the implementation setup created for thecore research work.

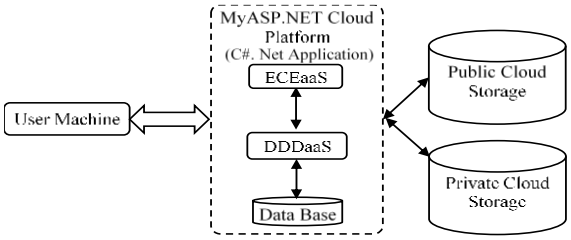

Figure 5 Implementation set up for the core research work

Convergent encryption, convergent encryption key generation and tag generation all these procedures are all running in the developed cloud-based application. This paper considers the running time of the ESCET for encryption and decryption. The proposed algorithm is measured by two parameters, time and security of the data. Time is calculated from the execution of the ESCET procedure. The encryption and decryption time is calculated from the hosted application. Figure 6 shows the time comparison of proposed and existing encryption techniques. The comparison shows for different sizes of data. From the result, it is noticed that the proposed ESCET consumes minimum time to encrypt the data.

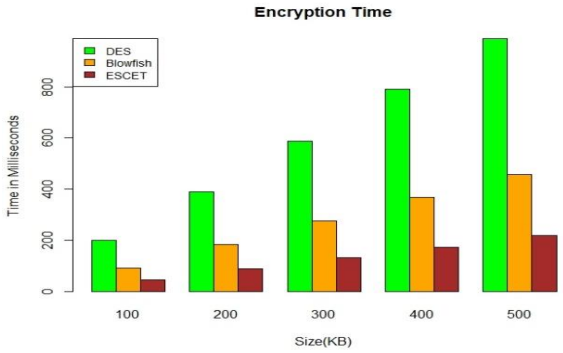

Figure 6 Encryption time caused by the Proposed and Existing Techniques

Figure 7 shows the time comparison of proposed and existing encryption techniques concerning decryption time. The comparison shows the time taken for different sizes of data. From the result, it is noticed that the proposed ESCET consumes minimum time to decrypt the data.

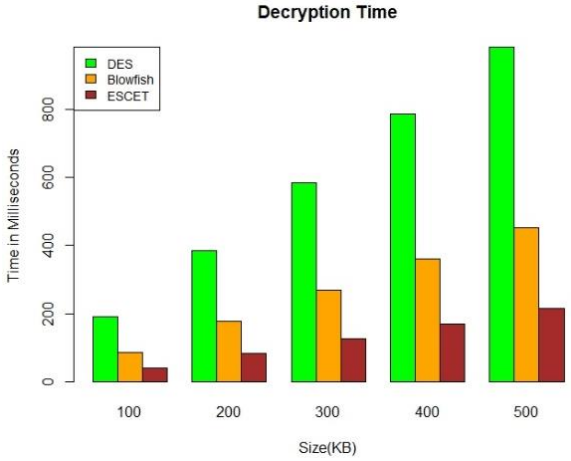

Figure 7 Decryption time caused by the Proposed and Existing Techniques

The security of the proposed technique is measured by using a hacking tool called the ABC Hackman tool. This tool is used to measure the security level of the encryption technique in percentage. The Hackman Tool has a robust library that contains many packages for different existing encryption techniques and attacks. The proposed technique is also deployed as a legacy package in the Hackman tool library. The tool receives input as encrypted data generated by the ESCET. The encrypted data is attacked using brute-force and dictionary attacks to retrieve the original plaintext data. According to the retrieved data by the Hackman tool, the security level is calculated using the formulas below.

The steps to be considered to measure the level of safety of proposed and existing techniques are:

Let N be the total amount of encrypted text stored in the cloud storage, X is the amount of original text extracted from the encrypted text by ABC Hackman.

For measuring the level of security,

$$K = N - X \quad (1)$$

Where K is the amount of text that does not match the original text.

The percentage of the security level is thus measured as follows:

$$Z = \frac{K}{N} * 100 \quad (2)$$

Where Z indicates the percentage of the security level of the proposed and existing encryption technique, and the percentage of the security level is measured by,

$$Y = \frac{X}{N} * 100 \quad (3)$$

Where Y indicates the percentage of insecurity level of the proposed algorithm and the existing technique, each technique generates a different level of security depending on its working procedure.

Figure 8 shows the security of the encryption techniques. The security level is an analyst by the method given above. In addition, the ABC Hackman tool is used to get the security level of the proposed and existing techniques. The results revealed in the table and figure clearly state that the proposed ESCET provides maximum security compared to the other encryption techniques.

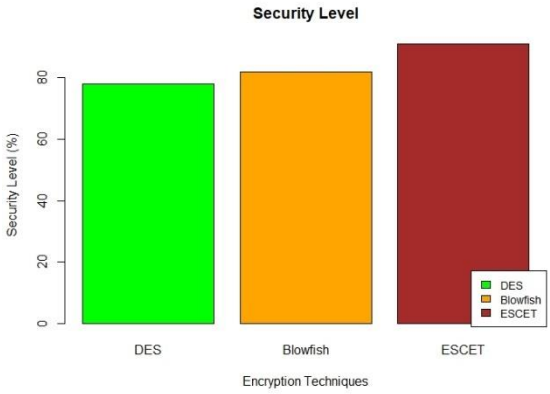

Figure 8Security Level of the Proposed and Existing Techniques

7.Conclusion

Cloud computing is a profitable computing service for individuals and businesses.However, some individuals may be hesitant to use it due to safety issues.Once the issues are resolved, the cloud will be the activity of trillions of dollars in the computer world.In addition, data storage on an unreliable cloud raises a data security concern.However, the confidentiality of sensitive data ensures that the data in the cloud is secure.

Along with security issues in cloud storage, data duplication is also the top concern to address. The paper proposed an enhanced symmetric convergent encryption technique to address cloud storage's security and deduplication issue. The proposed technique is symmetric encryption with the convergent approach, which helps to eliminate duplicate data in cloud storage. The research work proposed in the paper is one of the core research work. The deduplication mechanism and key generation service in the core research framework support the proposed work in this paper. The proposed work is implemented in the real-time cloud platform called MyASP.NET. ESCET is compared with other techniques based on the time and security level. The tables and graphs show the result of the proposed technique. Based on the results obtained, it is observed that the ESCETperform well and provides greater security to data inthe cloud.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. 2021;IEEE Access(9):57792-57807.

[2] D. Zhang, J. Le, N. Mu, J. Wu and X. Liao. Secure and EfficientData Deduplication in JointCloud Storage.2021;IEEETransactions on Cloud Computing:1-12.

[3] Manikandasaran, S. S., K. Balaji, and S. Raja. Infrastructure Virtualization Security Architecture Specification for Private Cloud. International Journal of Computer Sciences and Engineering.2018; 6(2): 10-14.

[4] Zahra Pooranian, Member, IEEE, Mohammad Shojafar, Senior Member, IEEE, Sahil Garg, Member, IEEE, Rahim Taheri and Rahim Tafazolli, Senior Member, IEEE. LEVER: Secure Deduplicated Cloud Storage with Encrypted Two-Party Interactions in Cyber-Physical Systems. 2020; IEEE: 1-10.

[5] Manikandasaran, S. S., and L. Arockiam. Security Attacks and Cryptography Solutions for Data Stored in Public Cloud Storage. IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS).2016; 2249-9555.

[6] Manikandasaran, S. S., Lawrence Arockiam, and PD Sheba Kezia Malarchelvi. MONcrypt: a technique to ensure the confidentiality of outsourced data in cloud storage. International Journal of Information and Computer Security. 2019; 11(1) : 1-16.

[7] Aparna Manikonda, Nalini N. Fine-Grained Security in Cloud with Cryptographic Access Control. International Conference on Advanced Computing and Innovative Technologies in Engineering (ICACITE).2021; IEEE:154-157.

[8] Wang Xiaoyu, Gao Zhengming. Research and Development of Data Security Multidimensional Protection System in Cloud Computing Environment, International Conference on Advance in Ambient Computing and Intelligence (ICAACI).2020; IEEE; 67-70.

[9] Priteshkumar Prajapati, Parth Shah. A Review on Secure Data Deduplication: Cloud Storage Security Issue. Journal of King Saud University .Computer and Information Sciences.2020; Elsevier;1280-1283.

[10] Laura Conde-Canencia, Belaid Hamoum. Deduplication algorithms and models for efficient data storage. International Conference on Circuits, Systems, Communications and Computers (CSCC).2020; IEEE:23-28.

[11] L. Suresh and M. A. Bharathi. Analysis of Block-Level Data Deduplication on Cloud Storage. Ambient Communications and Computer Systems, Advances in Intelligent Systems and Computing 904, Springer Nature Singapore.2019; 401-409.

[12] Y. Zhang, C. Xu, N. Cheng and X. S. Shen. Secure Password-Protected Encryption Key for Deduplicated Cloud Storage Systems. IEEE Transactions on Dependable and Secure Computing.2021;1-14.

[13] Infall Syafalni, Hamdani Fadhli, Wuri Utami, Gede Satya Adi. Cloud Security Implementation using Homomorphic Encryption. International conference on communication, Networks and satellites (Comnetsat).2020; IEEE:341-345.

[14] Yoshita Sharma, Himanshu Gupta, Sunil Kumar Khatri. A Security Model for the Enhancement of Data Privacy in Cloud Computing. 2019;IEEE; 898-902.

[15] Jianting Ning, Xinyi Huang, Willy Susilo, Senior Member, IEEE, Kaitai Liang, Member, IEEE, Ximeng LiuMember, IEEE, and Yinghui Zhang, Member, IEEE. Dual Access Control for Cloud-Based Data Storage and Sharing.2019; IEEE:1-13.

[16] Jian Wang, Chunxiao Ye, Yangfei Ou. Dynamic Data Access Control for Multi-Authority Cloud Storage. 2019; IEEE:599-608.

[16] Soumalya Ghosh, Anubhav Raj Singh, Garima Pandey, Anupam Lakhanpal. A Novel Solution to Cloud Data Security Issues. International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).2020; IEEE:857-860.

[18] Adesh Kumari, M. Yahya Abbasi, Mansaf Alam. A smartcard-based key agreement framework for cloud computing using ECC. International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV).2021; IEEE:43-48.

[19] Yogita Deepak Sinkar, C.Rajabhushnam. Data Protection on Cloud Using GWOA Model. International Conference on Computer Communication and Informatics (ICCCI). 2021; IEEE:1-5.

[20] Arfatul Mowla Shuvo, Md. Salauddin Amin, Promila Haque. Storage Efficient Data Security Model for Distributed Cloud Storage. 2021; IEEE:1-6.

[21] Magesh Kumar S, Balasundaram A, Kothandaraman D, Auxilia Osvin Nancy V, P. J. Sathish Kumar, Ashokkumar S. An Approach to Secure Capacity Optimization in Cloud Computing using Cryptographic Hash Function and Data De-duplication. International Conference on Intelligent Sustainable Systems (ICISS). 2020: IEEE:1256-1262.

[22] Dr B. Tirapathi reddy, Maddireddy Vaishnavi, Makireddy Lalitha, Papineni Poojitha, Vakalapudi Bhavya Sri Kanthi. Privacy-Preserving Data Deduplication in the cloud using Advanced Encryption Standard. International Conference on Artificial Intelligence and Smart Systems (ICAIS).2021; IEEE: 1205-1210.

[23] Haoran Yuan, Xiaofeng Chen, Senior Member, IEEE, Jin Li, Tao Jiang, Jianfeng Wang, and Robert H. Deng, Fellow, IEEE. Secure Cloud Data Deduplication with Efficient Re-encryption. Transactions on Services Computing.2019; IEEE: 1-14.

Balaji. K is a Research Scholar in PG and Research Department of Computer Science,Adaikala Matha College, Vallam, Thanjavur, Tamil Nadu, India. He has 12 years of experience in teaching. He completed his MCA in Dr.M.G.R University, Chennai, in 2006. M.Phil in Vinayakamission University, Salaem in 2009, and ME in Arunai Engineering College, Affliated with Anna University, Chennai in 2015.His research interest is Cloud computing, Network Security, Cloud Security, IoT, and Web Technology.
Email:balajjee.mecse@gmail.com

Manikandasaran S. S. is working as Associate Director in PG and Research Department of Computer Science, Adaikala Matha College, Vallam, Thanjavur, Tamil Nadu, India. He has 14 years of experience in teaching and 13 years of experience in research. He completed his MCA and M.Tech in Bharathidasan University, Tiruchirappalli, in 2007 and 2009, respectively, and completed his PhD in Manonmaniam Sundaranar University Tirunelveli in 2015. Now he is pursuing Post Doctoral Fellowship at Srinivas University, Karnataka,India. He has attended many International and National Conferences, Seminars, and Workshops. He has published 56 research articles in the International / National Conferences and Journals. He has delivered more than 45 lecturers in various National and International level seminars, workshops, and conferences. He is a author of a book. He has published two Indian Patent. His research interest is Cloud computing, Network Security, Cloud Security, IoT, and Web Technology.
Email:ssmanikandasaran@gmail.com