DOUBLE SIGNATURE BASED CRYPTOGRAPHY USING DS-SHA256 IN CLOUD COMPUTING

K. Prathapkumar[1], Dr. A. Thirumurthi Raja[2]

[1]Research Scholar, Email: prathapmcadept@gmail.com
[2]Research Supervisor & Assistant Professor, Email: dr.a.thirumurthiraja@gmail.com
Department of Computer Science, School of Computing sciences, Vels Institute of Science Technology and Advanced Studies (VISTAS), Chennai.

Abstract

Technology advancement and quick progressing have become vital in recent years. Cloud technology is one among them which has rapid growth in various domains. But a serious concern is data privacy and data security of the valuable data stored in cloud storage. The main reason for this untrustworthiness is Cloud Service Provider (CSP) because CSP is a third-party vendor. In this research work, double encryption algorithm using SHA256 with RSA known as DS-SHA256 is proposed. A double digital signature scheme was introduced in the proposed system. It achieves enhanced security with minimum consumption considering the existing works. To prove the efficiency of the proposed DS-SHA256, comparison work is carried out between the existing RSA and AES. The obtained result proved that the proposed DS-SHA256 security level and overall performance are far better than the others.

Keywords: Encryption, Decryption, RSA, AES, Cloud technology, Cloud Service Provider (CSP)

INTRODUCTION

The technology advancement and evolution of internet services with computer networking know as the cloud. Cloud computing has rapidly grown in recent years with its salient features like resources with rapid elasticity, quality services, consistent service, and remote access to the network. The existing traditional technology fails to achieve successful data outsourcing process. In cloud computing, data outsourcing is a significant process. Cloud data outsourcing includes storing huge data and sharing Information Technology (IT) vendors with minimum expense.

Cloud storage is well known for its enhanced efficiency and minimum utilization cost, which is prominent among other technologies. The cloud storage comprises several pools that maximize the computing services known as "software as a service". The remote data center facilitates the user to access the data from anywhere and anytime through a high-quality network connection [1]—Jaidi et al. [2] analysis about the higher-level integrity of access control policies. The traditional storage technologies fail to provide massive storage space and can be accessed anywhere geographical locations like cloud storage. The cloud storage allows cloud users to use any network type with any devices and the only things internet connection. Cloud storage has various salient features, but still, data security is a challenging problem. The enormous amount of increased cloud users and its wide entities makes data security a most complex and challenging task. Hence its makes addressing and overcoming the data security breaches an essential one. The cloud users can avail the cloud services through Cloud Service Provider (CSP). The CSP is the third-party cloud service provider that will facilitate the services as per the user requirements.

The CSP has its security policies while delivering a service to an authorized cloud user. The primary reason for trustworthiness in cloud storage is the user stored their sensitive data securely, but the storage space provided by CSP is a third-party vendor. It makes possible for various attacks including virtual machine side-channel attack [3]. Even though the cloud framework is structured with high-security features, the data loss problem occurs frequently. Sometimes, the data which are not used often by the user is eliminated by the CSP. The user stored information is still available even it is deleted [4, 5]. These are the common issues that cloud users faced. These issues questioned the individual cloud user to use the cloud services and drained the cloud popularity globally.

The vital process in the cloud service is verification; it ensures data integrity and data authentication in the cloud environment. The verification process had a significant impact in minimizing the data theft vulnerabilities. The third-party auditing process is the traditional public verification process used for verifying stored data in cloud storage [6]. The traditional public verification process is implemented in several security models [7]. The third-party auditing process involves authenticating and communicating the collected information in ensuring data integrity. The Third-Party Auditor (TPA) process does not need to reveal with the cloud user. The TPA will share the detailed auditing report to the cloud user with the user's stored data integrity verification history. There is no need for any extra efforts for the cloud users in employing and getting verified data. The efficient TPA process includes not introducing any issues to the cloud users and not getting any copy of user data.

The electronic document is the process of digital signature shared to the receiver, ensuring the documents genuine. The digital signatures replace the analog signature. There are two reasons for this one is digital signature is unique, which prevents duplication. Secondly, the analog signature is the same for individual users in all documents, but it is different for digital signatures. The digital signature differs according to the specific document information. The digital signature algorithms are based on discrete logarithms. The digital signature process executes four services: data integrity, Peer entity authentication, data origin authentication, and non-repudiation.

RELATED WORK

Yong et al. (2012) [8] developed a homorphic encryption mechanism to improve CSP's data security. AWS is a public cloud where data are stored through a shared resources pool. Based on shared EC2 instances, the data are stored in the cloud. The user with his machine will process the data, and it is encrypted when stored in the public cloud. Improvisation of cloud security is the only way to avoid data leaks in the cloud. There are various crypto algorithms and hashing techniques are evolved to maximize security. Some of the few known data security mechanisms are image encryption, captcha mechanisms, serverless encryption, and serverless computing. Kumari et al. (2018) [9] and Xiong et al. (2018) [10] approach virtualization mode-based security mechanisms. Using RSA public key, private key, encryption, and decryptions are processed virtually and physically. Algarni .et al(2019) [11] applied advanced encryption standards (AES) to address the cloud's data security issues. Additionally, symmetric and asymmetric algorithms are used to achieve security in all cloud applications. The cloud manager is responsible for managing the security patches, and it is installed based on the customer requirements on updates. Li et al. (2017) [12] presented the binary algorithms for achieving cloud security. It is the combination of the algorithm used for detecting the dragonflies' mirrors and swarm knowledge.

The framework developed for cloud security is based on a multi-cloud environment for storing the data digitally. In which segmentation approach is implemented for avoiding data disclosure. The segmentation approach fragments the input data into various areas. The outsourced client data integrity helps in validating watermarking techniques. This watermarking technique and digital signatures detect any accidental change to the outsourced client's data [13]. In this article[13] , the author described various methods' computation and data security performance against data breaches and security attacks. In this paper, mitigation methods like HMAC (Hashed Message Authentication Code) are discussed. The ECC and MD5 are used for achieving integrity, authentication, confidentiality, and access control as the security solution for real cloud computing environments. As a result, minimum overhead on upload and download service time is taken [14]. This work [15] presented a secure framework providing additional privacy to the cloud data. The framework is divided into various blocks of bit. A genetic algorithm is applied on every two blocks of bits. Each genomic algorithm procedure is concluded as an output of ciphertext with two blocks of bits. In the cloud, each ciphertext is stored at a distinct location, and the location is not secure. To increase the security on the framework, a genetic algorithm is implemented on minor block size. Additionally, a proficiency list enhances secure access to data.

In this article [16], a new framework is proposed to enhance data integrity and security. The encryption and decryption techniques have a more significant impact on achieving data security. The proposed mechanism not only achieves security but also increases the overall performance. It includes the processing of real-time monitoring, malware detection, and forensic virtual machine. In this article [17], the author discussed the framework and its objective in storing the data on clouds. The proposed framework is based on 3DES and RSA encryption. But it has the weakness of lack in privacy, efficiency, and overload issues on multiple functions. In [18], the author discussed the multilevel licensing framework for penetrating cloud data. The three covers' framework is responsible for safeguarding the delicate cloud data. The three films' security framework applies safety and approval policies, overload restrictions, and security and privacy strategies. In [19], the author proposed a quality-based cloud service broker framework (QCSB) by enforcing the metric standards on cloud service providers. But the implementation of QCSB consumes more effort. Finally, the author disclosed that the proposed material QCSB does not assist cloud computing to CSPs. **(8863345-related-work)**

Problem Analysis

The traditional cryptographic technologies are failed to address the following issues;

1) High cost
2) High time consumption for performing encryption and decryption.

These issues can be overcome by data partition, which minimizes the cost, reduces storage space, and enhances overall performance efficiency. Some of the common security and privacy-related problems in the cloud environment are listed below.

- ***Access control***: Internally, CSP failed to enable enhanced security mechanisms, resulting in unauthorized users accessing the stored data. It maximizes the possibility of intruders accessing the data simply.
- ***Authentication and Identification***: Several users requesting data access at a time lead to authentication and identification problems.
- ***Availability***: At all times, the requesting cloud service is not available for all users.
- ***Unauthorized usage & control policy***: This is the most critical issue because various CSP has various security mechanisms. On this occasion, CSP may lead to the leak of user data without the user's permission.

PROPOSED WORK

Contribution

In this research work, a double signature mechanism using SHA256 with RSA is introduced. This approach overcomes the drawbacks of the existing mechanism in the aspect of cloud security. After the encryption process, the CSP initiates the signature two times and stores the data in the cloud. The user can view the original data and get the data from CSP by passing two signatures and process decryption using the private key. RSA is a popular asymmetric algorithm, and its efficiency is improved with SHA256. The proposed implementation is straightforward and effective in comparison to the existing systems.

Objective

The main objective of this paper is to deliver complete data security and privacy for cloud storage. Figure1 illustrates the proposed architecture and its workflow clearly. The components of the proposed system are explained below;

Data Authority:

Data authority is responsible for creating or collecting the data in text, images, audio, and video. Data authority owns collected data in the cloud platform and is shared with various cloud users if needed. Data authority collected information need to be secured and preserve from unauthorized cloud users. This can be achieved by validating every end user's certificate who is requesting data. The credentials are verified, and the user is approved as authorized users, which means they can access the cloud-stored data.

Cloud Storage:

Cloud storage is a type of cloud service offered by the CSP. In which the authorized user can store and retrieve the data from anywhere anytime through the internet. The data stored in the cloud can be managed, preserved, and backup. The popular public cloud storage providers are Windows Azure, Amazon Elastic Compute Cloud (EC2), Sun Cloud, and Amazon's S3. This allows the user to store and transfer the data without any cost. The CSP enables additional features on the private cloud at cost based on the user requirements. It contains various features like reliability, confidentiality, and availability at minimum cost [11, 27].

Cloud Service Provider (CSP):

The cloud service provider (CSP) manages the essential data storage service and facilities storage place with some computational resources. The CSP provides some storage service to the cloud user, based on which the user can access/retrieve the corresponding data. The CSP took over the control of cloud data storage and servers. The virtual infrastructure performs the host application process.

End Users:

The end-user is the essential component of cloud computing services. The CSP that provides the cloud environment needs to satisfy the end-user requirements highly reliable and easily accessible. The data authorities provide some permission for the end-users based on they can process the stored data. The consent includes reading/writing on the e-stored revised data.

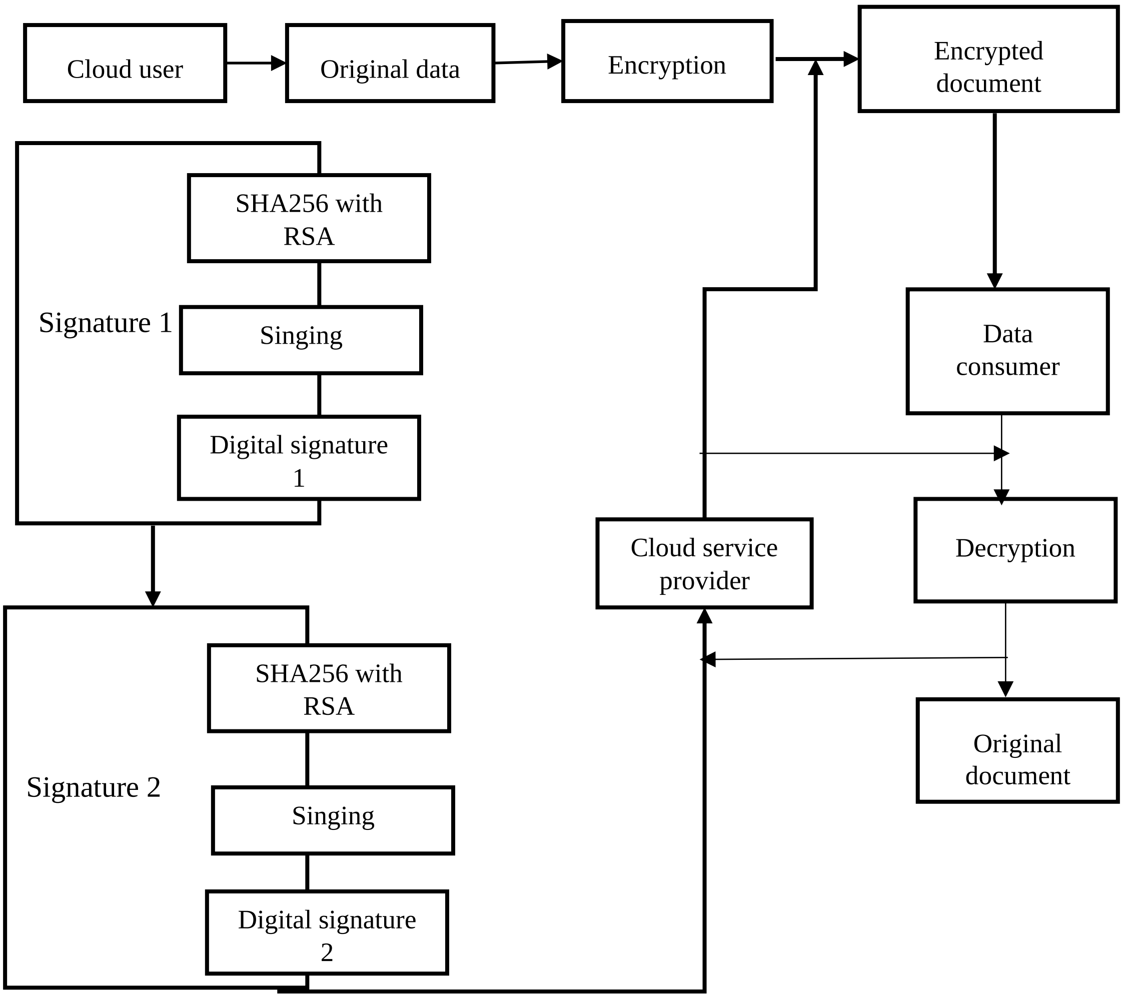

Figure 1 Proposed Architecture

Working principle

The above figure1 illustrates the proposed architecture, in which the user initially registered to the CSP for availing the services. Once the registration is successful, the cloud user can do the operation in the cloud environment. In this work, security on data storage is discussed with the implementation of the proposed system. The original data to be stored in the cloud is text, images, audio, and video. The data of its type is considered the original data, and before storing the data in the cloud, it gets encrypted. Encryption is the process of converting plain text into cipher text. To preserve the data privacy, the proposed system introduces a double signature mechanism. According to which the initially the data is encrypted and passed to the data consumer. For availing of the storage service, the cloud user first encrypts the data using SHA256 with RSA. It is a symmetric algorithm that contains public and private keys. Once the user encrypted the data its passes to the CSP with digital signature 1. Again, CSP did the second encryption with digital signature 2 and stored the data in the cloud. If the user wants to retrieve the original data, he/she will have sent a request to the data consumer. The data consumer valid the digital signature of the request, and if it's valid, then allows accessing the stored data in CSP. The user needs to provide the private key which he/she has obtained during encryption, and based on that, the decryption is done to get the original data. Decryption is the process of converting the cipher text into the plain or original text. The step by step implementation of the proposed algorithm is explained below;

DSSHA256 with RSA

Step 1: Read the original document, which is to be stored in the cloud database.
Step 2: The sender uses a signing algorithm to sign the message. The message and the signature are sent to the Cloud Server.
Step 3: Key Generation
a) A prime p between 512 and 1024 bits in length is chosen. The number of bits in p must be a multiple of 64.
b) A prime q of 160 bit is chosen such that it divides (p-1).
c) A primitive element in Zp is chosen and e1 = e0(p-1)/q mod p is calculated.
d) d is chosen as the private key, and e2 = e1d is calculated.
Public key – (e1, e2, p, q)
Private key – d
Step 4: Double Signature
1. A random number r is chosen such that (1 <= r <=q). New r needs to be chosen each time to sign a new message.
2. The first signature S1 = (e1r mod p) mod q. The value of the first signature does not depend on M.
3. The second signature S2 = (M +dS1) r-1 mod q.
Step 5: Encrypted Document will be sent to cloud Server.
Step 6: Data Consumer initialize the document request
Step 7: Signature Verification
1. 0 < S1 < q is checked.
2. 0 < S2 < q is checked.
3. V = [(e1h(M)S2-1 e2S1S2-1) mod p]mod q
4. If S1 is congruent to V, message is accepted otherwise rejected.

Experimental results

In this section, experimental work is carried out to describe the performance of the proposed DS-SHA256. The obtained result is compared with the existing AES and RSA techniques. The experimental setup includes an Intel(R) Core(TM)2 Duo CPU processor with a Windows 7 platform of 4GB RAM and Java programming. The evaluation metrics taken for comparison are Encryption time and Decryption time. The obtained result from each algorithm is plotted in graphical representation for performance discussion among them.

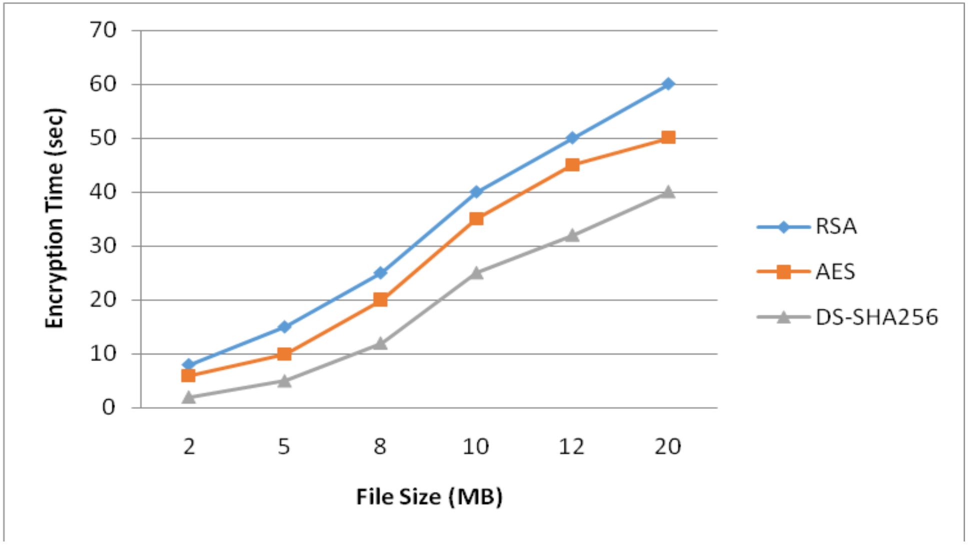

Figure 2 Encryption time Vs. File Size

The Figure 2 illustrates the observation on encryption time achieved with various loads by RSA, AES, and proposed DS-SHA256. The y-axis represents the encryption time which is measured in sec. The x-axis represents the file size upload for encryption in terms of MB. The file size is increased gradually in the experiment. The proposed DS-SHA256 achieves encryption of 2MB file in 0.2 secs, 5MB file in 0.5 secs, 8MB file in 12 secs, 10 MB file in 24secs, 12MB file in 31 secs, and 20MB file in 40 secs. The graphical representation clearly shows that the proposed DS-SHA256 is far better than the existing RSA and AES in all workloads.

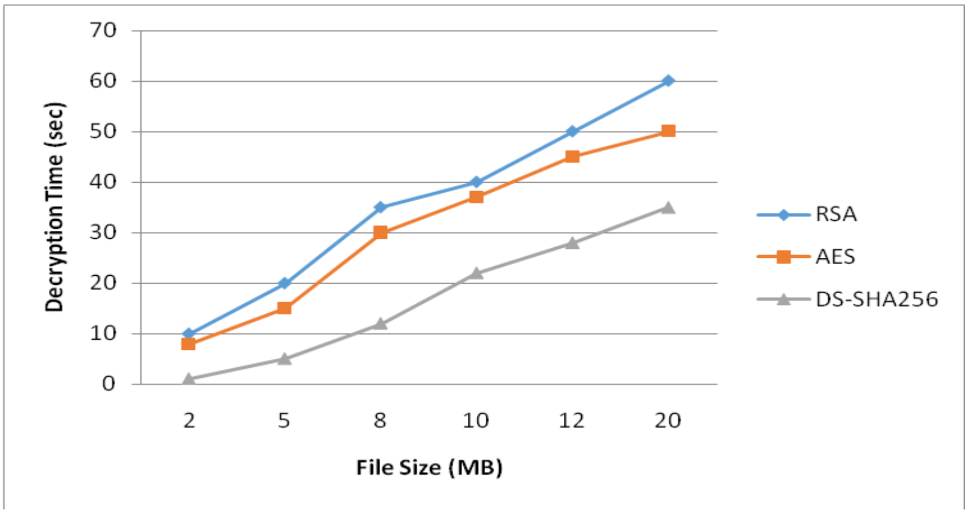

Figure 3 Decryption time Vs. File Size

The Figure 3 illustrates the observation on decryption time achieved with various loads by RSA, AES, and proposed DS-SHA256. The y-axis represents the decryption time which is measured in sec. The x-axis represents the decrypted file size in terms of MB. The file size is increased gradually in the experiment. The proposed DS-SHA256 achieves decryption of 2MB file in 0.1 secs, 5MB file in 0.5 secs, 8MB file in 12 secs, 10 MB file in 24secs, 12MB file in 28 secs, and 20MB file in 35 secs. The graphical representation clearly shows the decryption performance of the proposed DS-SHA256 more efficiently than the existing RSA and AES in all workloads.

CONCLUSION

In this research article, the importance of cloud storage security is discussed in the view of cloud users. Cloud trustworthiness is a major key for the growth of cloud services globally. In the cloud, cryptography is the only approach for achieving data security. It includes two processes of such as encryption and decryption. Various security mechanisms are evolved, but they are inefficient to perform encryption and decryption effectively and overall performance. Double encryption scheme using SHA256 with RSA known as DS-SHA256is proposed here. It contains a double signing system under the supervision of CSP. To validate the performance of the proposed system, a comparison work is carried out between the proposed DS-SHA256 with the existing RSA and AES. The performance metric taken for consideration is Encryption time and Decryption time under various workloads. In all the cases, the proposed system is more prominent and illustrates the enhanced security metrics and performance efficiency than the existing RSA and AES.

REFERENCE

1. Rivest R., Shamir A., and Adleman L., “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.
2. Jaidi F., Ayachi F., and Bouhoula A., “Advanced Analysis of the Integrity of Access Control Policies: the Specific Case of Databases,” The International Arab Journal of Information Technology, vol. 17, no. 5, pp. 808-815, 2020
3. Stallings W., Cryptography and Network Security: Principles and Practice, Prentice Hall, 2011
4. Li T., Liu Z., Li J., Jia C., and Li K., “CDPS: A Cryptographic Data Publishing System,” Journal of Computer and System Sciences, vol. 89, pp 80-91, 2017.
5. Perbawa M., Afryansyah D., and Sari R., “Comparison of ECDSA and RSA Signature Scheme on NLSR Performance,” in Proceedings of IEEE Asia Pacific Conference on Wireless and Mobile, Bandung, pp. 7-11, 2017
6. Kaaniche N. and Laurent M., “Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms,” Computer Communications, vol. 111, pp 120-141, 2017
7. Kumar S., Kumar M., Budhiraja R., Das M., and Singh S., “A Cryptographic Model for Better Information Security,” Journal of Information Security and Applications, vol. 43, pp. 123-138, 2018.
8. Yong P, Wei Z, Feng X, Dai Z-H, Yang G, Chen D-Q (2012) Secure cloud storage based on cryptographic techniques. J China Univ Posts Telecommun 19:182–189
9. Kumari S, Karuppiah M, Das AK, Li X, Wu F, Kumar N (2018) A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74:6428–6453
10. Xiong H, Zhang H, Sun J (2018) Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing. IEEE Syst J.
11. Algarni A (2019) A survey and classification of security and privacy research in smart healthcare systems. IEEE Access
12. Li Y, Gai K, Qiu L, Qiu M, Zhao H (2017) Intelligent cryptography approach for secure distributed big data storage in cloud computing. Inf Sci 387:103–115
13. M. Marwan, A. Kartit, and H. Ouahmane, “A framework to secure medical image storage in cloud computing environment,” Journal of Electronic Commerce in Organizations, vol. 16, no. 1, pp. 1–16, 2018.
14. J. Silki and V. Abhilasha, “An improved security framework for cloud environment using ECC algorithm,” International Journal for Research in Applied Science & Engineering Technology, vol. 6, no. 1, 2018.
15. A. Oussama and Z. Abdelha, “A security framework for cloud data storage (CDS) based on agent,” Applied Computational Intelligence and Mathematical Methods, Springer, Berlin, Germany, 2019.
16. P. Sirohi and A. Agarwal, “Cloud computing data storage security framework relating to data integrity, privacy and trust,” in Proceedings of the 2015 1st International Conference on Next Generation Computing Technologies (NGCT), pp. 4-5, Dehradun, India, September 2015.
17. K. Subramanian, F. L. John, and F. L. John, “Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system,” International Journal of Advanced and Applied Sciences, vol. 5, no. 1, pp. 15–23, 2018.
18. H. J. Muhasin, R. Atan, M.A. Jabar, and S. Abdullah, “Cloud computing sensitive data protection using multi layered approach,” in Proceedings of the 2016 2nd International Conference on Science in Information Technology (ICSITech), pp. 69–73, Balikpapan, Indonesia, October 2016.
19. Arunachalam, A. S., and A. P. Hidhaya. "Locating nearest neighbor using privacy query based on improvised paillier cryptosystem." Journal of Advanced Research in Dynamical and Control Systems 5 176-182, 2017.
20. K. Ravi and K. B. Rajesh, “Quality based cloud service broker for optimal cloud service provider selection,” International Journal of Applied Engineering Research, vol. 12, no. 18, pp. 7962–7975, 2017.