https://doi.org/ 10.33472/AFJBS.6.10.2024.3819-3828

AFJBS

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Adaptive Service Centric Data Encryption Model for Improved Data Security in Cloud

Dr.F Rahman, Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India.
Mail ID:ku.frahman@kalingauniversity.ac.in
ORCID ID: 0009-0007-7167-188X

Omprakash Dewangan, Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India.
Mail ID:ku.omprakashdewangan@kalingauniversity.ac.in
ORCID ID: 0009-0003-1578-0708

Article History

Volume 6,Issue 10, 2024

Received:13 Apr 2024

Accepted : 05 May 2024

doi: 10.33472/AFJBS.6.10.2024.3819-3828

Abstract:

The data security in cloud has been identified as a key challenge for the organizations. To maintain the security level, various security check and encryption standards are used in literature. However, the methods compromise on security of data as the does not consider the cost of encrypting data, security performance and time complexity. To handle this issue, an efficient Adaptive Service Centric Data Encryption Model (ASCDEM) is presented. With the focus on securing the data by enforcing rigid encryption standards at service level. The method maintains number of services belongs to various categories which are classified into two cases based on their nature. The services are classified into impact services and non-impact services. Upon receiving the request, the method identifies the category of the service and computes Data Impact Weight (DIW) for the service as per the features access. Based on the value of DIW, the method identifies the subclass of the service. According to the service class identified, the method selects a optimal encryption scheme for the service. Encrypted data has been given to the user which can be reversed in the same way. The ASCDEM model records noticeable performance growth in data encryption and decryption with higher data security.

Cloud, Data Security, Encryption standards, ASCDEM, DIW.

Introduction:

The growth of information technology encourages the data world to maintain data in various data servers. However, the cost of data maintenance has become a huge challenge for the organization. Also, the security threat on the data being maintained is identified as key issue in modern informatics society. To solve this hectic situation, the cloud environment has arised as the solution for the organizations. The cloud service providers support the organizations in maintaining their data in cloud with least costs. The members of the organization are allowed to manipulate the data through set of services provided. In general, cloud is a loosely coupled environment where the service provider does not have enough knowledge about the people who access the service.

The nature of cloud encourages the adversaries in performing various service threats. The adversary would perform flooding attacks, guessing attack and others also. The ultimate aim of the adversary is to learn the data available in the cloud. To secure the data from such threats, apart from access restriction, the encryption schemes are used. The general encryption standards like AES, DES and ABE standards are effective on small scale problem. But they are highly compromise with the adversary and they can easily tamper the data. To safeguard the data present in the cloud, it is necessary to enforce dynamic approaches in cloud data.

With the intention to improve the data security performance, a Adaptive Service Centric Data Encryption Model (ASCDEM) is sketched in this article. ASCDEM model is focused on using different group of encryption standards which can be selected according to the data nature and service nature. If the service is accessing cloud data but does not perform any update then it can be classified as non-impact service. Again if the service is accessing some sensitive features then it can be classified as non-Impact-sensitive service. On the other side, if the service is accessing sensitive features and performing any update on the original data, then it can be classified as impact-sensitive service. By classifying the service, features under different classes, the encryption standards also can be grouped under various class to support the encryption process. The model receives the request and service data to compute the value of Data impact weight (DIW) to identify the class of service and based on that specific standard will be selected and data has been encrypted accordingly. This challenges the adversary in performing data stealing and modification attack towards improving data security.

The article is framed to present the detailed introduction on the problem in Section 1, and related topics with set of methods are explored in Section 2. Section 3, details the working of proposed method and evaluation results are described in section 4. Finally, section 5, details the conclusion of the work.

Related Works:

The methods of data security and data encryption are analyzed in this section.

A hybrid elliptic curve cryptography (HECC) scheme is presented in [1], towards data security in cloud. The method uses lightweight Edwards curve to generate the key and uses identity based encryption towards generating private keys. The method uses AES and Diffie Hellman towards key exchange and data encryption. A machine learning based symmetric searchable encryption scheme is presented in [2], which uses keyword ranking scheme with ANN to perform data encryption. A provable secure public key encryption scheme is presented in [3], which handles keyword guessing attack to encrypt data with private key and uses public key for verification. A bidirectional activation neural network is presented in [4], which maps the relationship with key and chaotic initial value to perform data encryption. A key aggregate searchable encryption with conjunctive queries (KASE-CQ) is presented in [5], which handles selective document chosen keyword attack. A triple data encryption standard (TDES) is presented in [6], which uses DES algorithm to perform data encryption with increased size of keys. A Revocable Identity-Based Broadcast Proxy Re-Encryption (RIB-BPRE) scheme is presented in [7], which address the key revocation issue and perform data encryption accordingly.

Multi data-Owner Searchable Encryption Scheme is presented in [8], which perform attribute based encryption by providing authorized key to perform data encryption with symmetric key encryption. The method uses different access policies to enforce efficient data access and security.

Multi-Keyword Searchable and Verifiable Attribute-Based Encryption is presented in [9], which performs verification with the use of Ciphertext Policy Attribute-Based Encryption (CP-ABE) scheme in a multi owner environment.

A Verifiable and Fair Attribute-Based Proxy Re-Encryption Scheme (VF-ABPRE) is presented in [10], which verifies the data obtained from the server is correct or not to perform data encryption effectively.

A Novel Revocable and Identity-Based Conditional Proxy Re-Encryption Scheme (RIB-CPRE-CE) is presented in [11], which combines the nature of fixed length cipher, fine grained authentication, and resistance security.

An Identity Based Proxy Re-Encryption Scheme is presented in [12], which performs data encryption by using keys shared between single hops.

A multi-proxy assisted revocable attribute group-based encryption (MP-RAGBE) scheme is presented in [13], which form user groups with similar attributes and shares keys to proxy server to support data encryption. A Dynamic Data Encryption Strategy (D2ES) is presented in [14], towards encrypting selective data as per timing features.

A Revocable Attribute Based Encryption with Data Integrity is presented in [15], which prove its confidentiality and integrity under the defined security model.

A Role-Based Encryption (RBE) Scheme is presented in [16], towards reducing cost overhead in data encryption.

The methods are inclined and compromised to produce expected performance in data security.

Adaptive Service Centric Data Encryption Model (ASCDEM):

The ASCDEM model receives the service request from the user initially. From the service request, the method identifies the nature of the service and set of features being accessed by the service. Based on the service nature as impact or non-impact and based on the feature types being accessed, the method computes the Data Impact Weight (DIW) measure. As per the value of DIW, the service class and sub class are identified. From the identified class, the method identifies a optimal encryption scheme for the service from the service pool. The service pool contains number of services and has been classified into different categories. The selected scheme has been used to perform data encryption and the scheme id has been given to the user to decrypt the data. The detailed working is presented in this section.

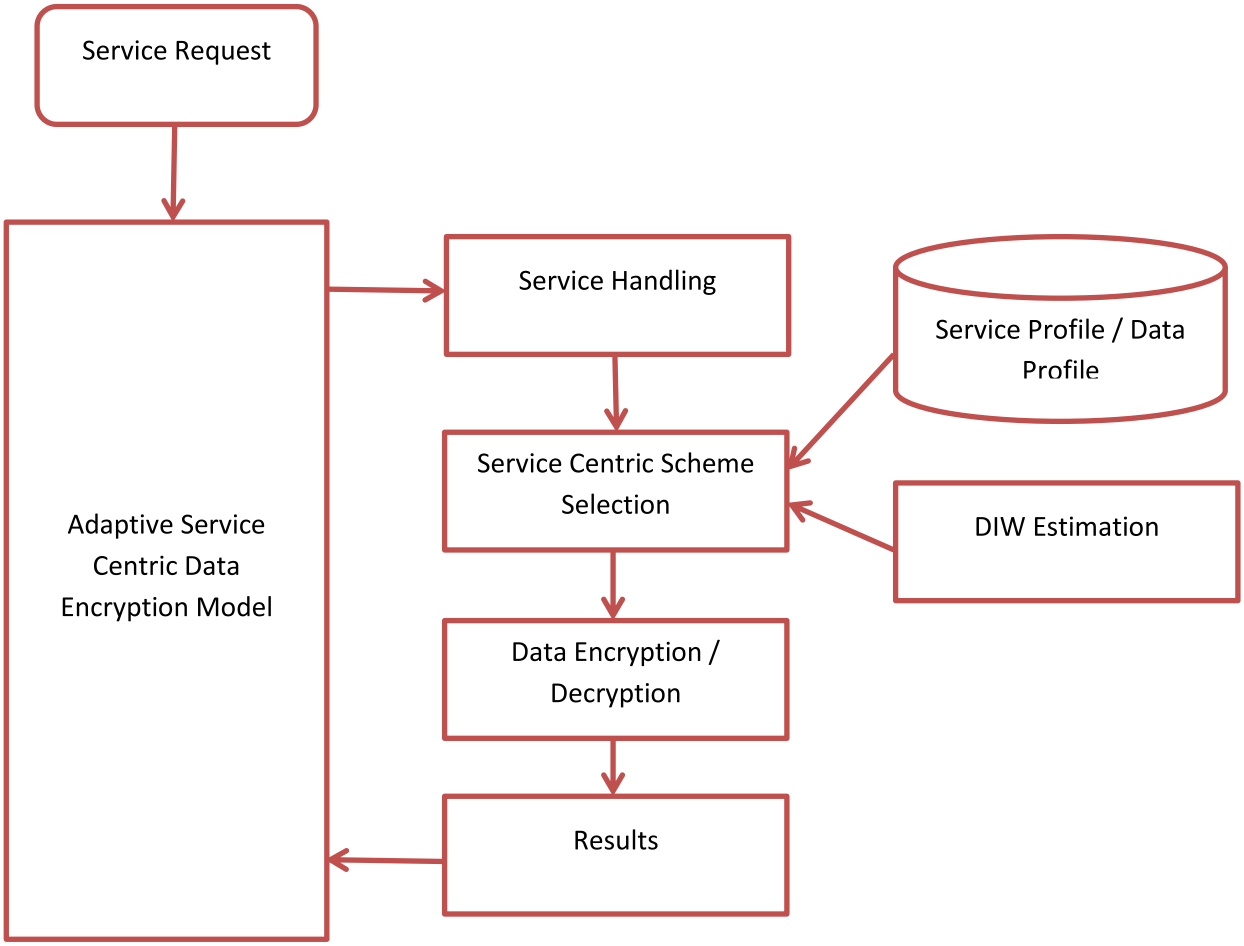
Service Request
Adaptive Service Centric Data Encryption Model
Service Handling
Service Profile / Data Profile
Service Centric Scheme Selection
DIW Estimation
Data Encryption / Decryption
Results

Figure 1: Architecture of Proposed ASCDEM Model

The working diagram of the ASCDEM model is sketched in Figure 1, and the stages are detailed in this part.

Service handling:

The service handling function is responsible of receiving the service request from the cloud users. From the service request received, the service type is identified and the set of features accessed by the service as well. Identified service and the features accessed are passed to the Service Centric Scheme Selection function. The result received from the service centric scheme selection function is used for encryption and decryption. The result has been given to the user as reply.

Algorithm:

```
Given: Service Request Sr, Service Profile Sp, Data Profile Dp
Obtain: Result
Start
    Read Sr, Sp, Dp.
    Identify service nature Sn = $\overset{size(Sp)}{\underset{i=1}{}} Sp(i).Nature?\,(Sp(i).Sid == Sr.Id)$
    Feature sets fs = $\sum_{i=1}^{size(Dp)} Dp(i).Features?\,(Dp(i).Id == Sr.Id)$
    If Sn.Type == Access then
        Encryption Scheme Es = perform Service Centric Scheme Selection (Sn, Fs)
        Cipher data Cd = Perform Data Encryption (Service Data, Es)
        Send Cd to user.
    Elseif Sn.Type == Update then
        Original Data Od = Perform Data Decryption (Service Data, Es)
        For each feature f
            If ServiceData(f) == Genuine then
                Flag = genuine
            Else
                Flag= malicious
            End
        End
        If flag==genuine then
            Update data.
        End
    End
Stop
```

The working of service handling process receives the user request and acts according to the service type and other factors.

Service Centric Scheme Selection:

The security of the entire model is greatly depending on the service selection scheme. By choosing rigid encryption scheme, the performance can be greatly improved. To perform this, the method receives the service nature and set of features being accessed. According to the service nature and type with the features, the method computes DIW value. Based on the DIW value, the method identifies the optimal encryption scheme. Selected scheme has been given as result to the service handling function to perform other activities.

Algorithm:

```
Given: Service nature Sn, Feature Set Fs, Service Id Sid, Data Profile Dp, Service Profile Sp.
Obtain:        Scheme S
Start
        Read Sn, Fs, Sid, Dp, Sp.
        DIW = Perform DIW Estimation (Sn, Fs, Sid, Dp, Sp)
        Service Class sc = $\underset{i=1}{\overset{size(Sp)}{Sp(i).class?Sp(i).nature == Sn\&\&Sp(i).impact < DIW >}}$
        Scheme s = $\underset{i=1}{\overset{size(Sp)}{Rand\big(Sp(i)\big)?Sp(i).class == Sc}}$
Stop
```

The service centric scheme selection function computes the DIW value for the given service and identifies the class of service. Based on the class of service, the method selects a encryption scheme according to the DIW and service class identified.

DIW Estimation:

The data impact weight measurement function computes the data impact weight for the service. It has been measured according to the type of function, feature types, number of features accessed. The service may access number of features which are fall under various categories like low impact, high impact, low sensitivity and high sensitivity. This method counts the number of features accessed, number of impact features and non-impact features accessed. Further, based on these features, the method computes the DIW value. Estimated DIW value has been given as reply to the calling function.

Algorithm:

```
Given: Data Profile Dp, Feature Set Fs, Service Nature Sn.
Obtain: DIW
Start
        Read Dp, Fs, Sn.
        Compute Impact Feature Count IFC = $\underset{i=1}{\overset{Size(Fs)}{Count(Fs(i).Type == Impact)}}$
        Compute Non-Impact Feature Count NiFC = $\underset{i=1}{\overset{Size(Fs)}{Count(Fs(i).Type == Non\_Impact)}}$
        Compute DIW =$( \frac{IFC}{Size(FS)} \times \frac{NiFC}{Size(Fs)}) \times Sn$
Stop
```

The data impact weight measurement algorithm computes the number of impact features and non-impact features accessed by the service. Based on the count values, the method computes the value of DIW to perform scheme selection.

Experimental Results:

The proposed Adaptive Service Centric Data Encryption Model (ASCDEM) has been implemented with Azure platform with Advanced Java. The performance of the model has been evaluated under the presence of different number of service class and users. The results obtained have been presented in this section.

Key	Value
Tool	Microsoft Azure, Advanced Java
Number of Service Classes	5
Number of Services	50
Number of Users	200

Table 1: Evaluation Details

The details of evaluation have been presented in Table 1, which has been used to measure the performance of the proposed model.

Data Security vs No of Services			
	10 Services	25 Services	50 Services
HECC	69	74	78
KASE-CQ	72	77	83
RIB-BPRE	75	79	87
ASCDEM	82	91	98

Table 2: Analysis on Data Security

The performance in data security obtained by different schemes with the presence of varying number of services in the environment is gauged and plotted in Table 2. The proposed ASCDEM model hikes higher security performance than other approaches.

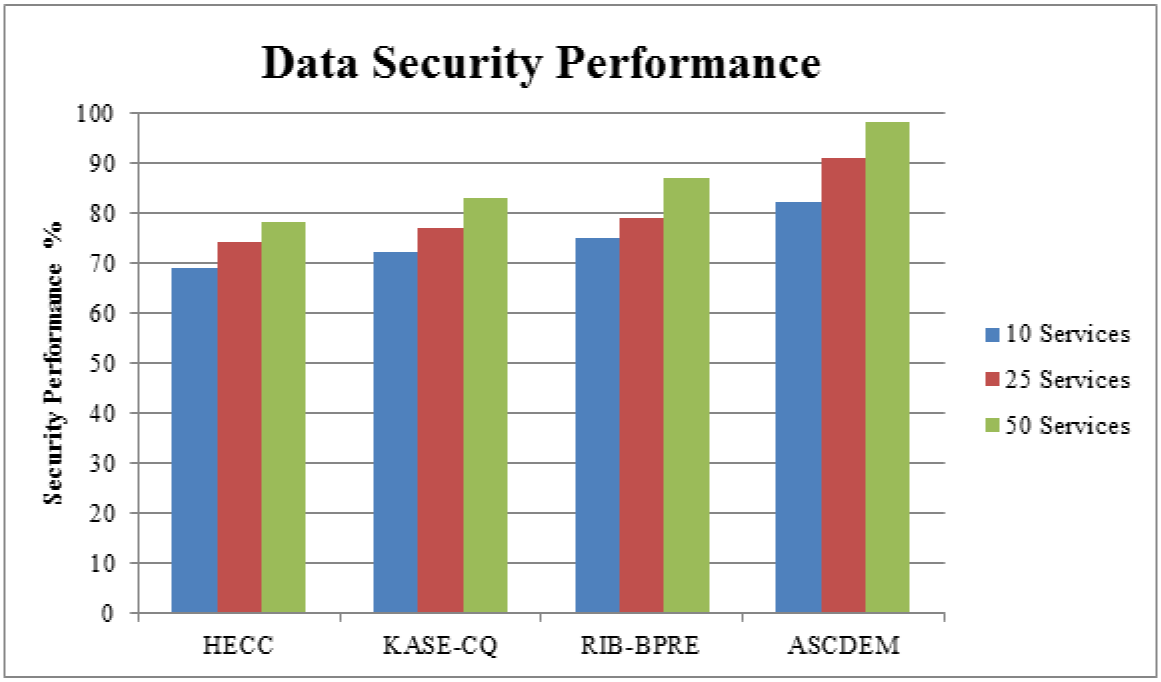

Figure 2: Analysis on Data Security vs No of Services

The data security efficiency of different schemes are measured and compared in Figure 2. The ASCDEM model introduces higher performance compare to others.

Encryption / Decryption Performance vs No of Services			
	10 Services	25 Services	50 Services
HECC	66	71	75
KASE-CQ	69	74	78
RIB-BPRE	73	78	83
ASCDEM	81	89	95

Table 3: Analysis on Encryption/Decryption Performance

The efficiency in encryption and decryption is evaluated and presented in Table 3. The ASCDEM model introduces higher performance than others.

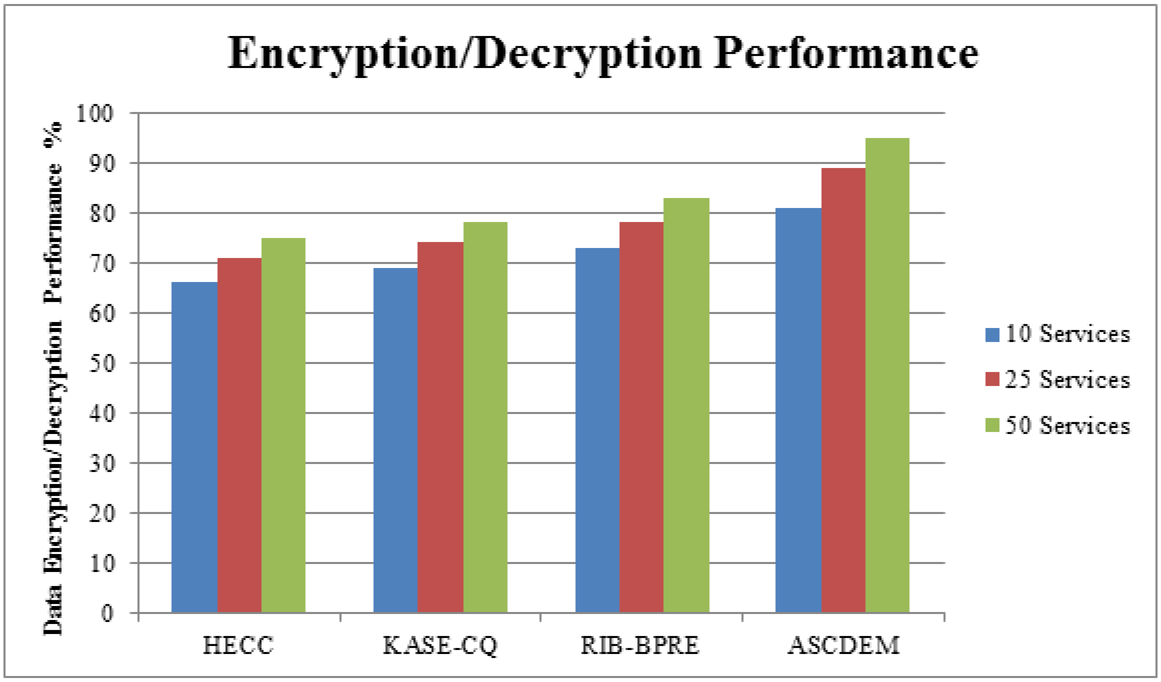

Figure 3: Data Encryption/Decryption Performance

The efficiency of methods in data encryption and decryption is evaluated and presented in Figure 3. The ASCDEM model produces higher performance than others. s

Conclusion:

This paper presented a novel Adaptive Service Centric Data Encryption Model (ASCDEM) towards security development in cloud. The model receives the user request and finds the service nature and set of features accessed. Using them, the method applies service centric scheme selection which in turn computes the DIW value for the service. Based on the DIW value, the method identifies the optimal service and performs encryption process. Similarly, for the update request, the method verifies the genuine of the feature and performs the process. The proposed method improves the data security and encryption/decryption performance.

References:

1. B. Ranganatha Rao," A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security", ELSEVIER (M:A), Volume 29, Number 100870, 2023.

2. Sheenam Malhotra, "An efficacy analysis of data encryption architecture for cloud platform", ELSEVIER (PCS), Volume 218, PP 989-1002, 2023.

3. Sudeep Ghosh, "Provably secure public key encryption with keyword search for data outsourcing in cloud environments", ELSEVIER (JSA), Volume 139, Number 102876, 2023.

4. Zhenlong Man, "Research on cloud data encryption algorithm based on bidirectional activation neural network", ELSEVIER (IS), Volume 622, PP 629-651, 2023.

5. Jinlu Liu, "Key-aggregate searchable encryption supporting conjunctive queries for flexible data sharing in the cloud", ELSEVER (IS), Volume 645, Number 119336, 2023.

6. Mohan Naik Ramachandra, "An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard", MDPI (BDCC), Volume 6, Issue 4, 2022.

7. C. Ge, Z. Liu, J. Xia and L. Fang, "Revocable Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," IEEE (TD&SC), Volume. 18, Number. 3, pp. 1214-1226, 2021.

8. S. Abdelfattah, M. Baza, M. M. E. A. Mahmoud, M. M. Fouda, K. A. Abualsaud and M. Guizani, "Multidata-Owner Searchable Encryption Scheme Over Medical Cloud Data With Efficient Access Control," IEEE (SJ), Volume. 16, Number 3, pp. 5067-5078, 2022.

9. Y. Zhang, T. Zhu, R. Guo, S. Xu, H. Cui and J. Cao, "Multi-Keyword Searchable and Verifiable Attribute-Based Encryption Over Cloud Data," IEEE (TCC), Volume. 11, Number 1, pp. 971-983, 2023.

10. C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia and L. Fang, "A Verifiable and Fair Attribute-Based Proxy Re-Encryption Scheme for Data Sharing in Clouds," IEEE (TD&SC), Volume. 19, Number 5, pp. 2907-2919, 2022.

11. S. Yao, R. V. J. Dayot, H. -J. Kim and I. -H. Ra, "A Novel Revocable and Identity-Based Conditional Proxy Re-Encryption Scheme With Ciphertext Evolution for Secure Cloud Data Sharing," in IEEE Access, Volume. 9, pp. 42801-42816, 2021.

12. S. Yao, R. V. J. Dayot, I. -H. Ra, L. Xu, Z. Mei and J. Shi, "An Identity-Based Proxy Re-Encryption Scheme With Single-Hop Conditional Delegation and Multi-Hop Ciphertext Evolution for Secure Cloud Data Sharing," IEEE (TIF&S), Volume. 18, pp. 3833-3848, 2023.

13. J. Cui, B. Li, H. Zhong, Y. Xu and L. Liu, "Achieving Revocable Attribute Group-Based Encryption for Mobile Cloud Data: A Multi-Proxy Assisted Approach," IEEE (TD&SC), Volume. 20, Number 4, pp. 2988-3001, 2023.

14. K. Gai, M. Qiu and H. Zhao, "Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing," IEEE (TBD), Volume. 7, Number 4, pp. 678-688, 2021.

15. C. Ge, W. Susilo, J. Baek, Z. Liu, J. Xia and L. Fang, "Revocable Attribute-Based Encryption With Data Integrity in Clouds," IEEE (TD&SC), Volume. 19, Number 5, pp. 2864-2872, 2022.

16. N. H. Sultan, V. Varadharajan, L. Zhou and F. A. Barbhuiya, "A Role-Based Encryption (RBE) Scheme for Securing Outsourced Cloud Data in a Multi-Organization Context," IEEE (TSC), Volume. 16, Number 3, pp. 1647-1661, 2023.

17. H. Hu, Z. Cao and X. Dong, "Autonomous Path Identity-Based Broadcast Proxy Re-Encryption for Data Sharing in Clouds," in IEEE Access, Volume. 10, pp. 87322-87332, 2022.

18. H. Song, J. Li and H. Li, "A Cloud Secure Storage Mechanism Based on Data Dispersion and Encryption," in IEEE Access, Volume. 9, pp. 63745-63751, 2021.