A Cloud Security Model for Document Retrieval by Applying CP-ABHE Scheme Using SNG Technique

Surendra Kumar Pathak

[1]Research Scholar, Department of Mathematical Sciences and Computer Applications,
Bundelkhand University, Kanpur Road, Jhansi, Uttar Pradesh, India.
e-mail: pathak.surendra@gmail.com
Orcid: https://orcid.org/0000-0003-0525-8994

Dr. Alok Kumar Verma

[2]Associate Professor, Department of Mathematical Sciences and Computer Applications,
Bundelkhand University, Kanpur Road, Jhansi, Uttar Pradesh, India.
e-mail: alokverma_bu@yahoo.com
Orcid: https://orcid.org/0000-0002-3477-5379

Article Info

Page Number: 7368 - 7383

Publication Issue:

Vol 71 No. 4 (2022)

Abstract

Cloud computing is an extremely vast field and is growing exponentially. During lockdown, everyone extensively used online tools to perform their day to day tasks like online classes, professional meetings, personal communication, etc., as well as store the meeting data. Security is a major concern in all these online activities. Cloud Computing or cloud services have played an important role in the entire scenario of security issues. Here, we initially perform cipher text policy hierarchical attribute based encryption technique (CP-ABHE) to encrypt the data. In the next stage, we have stored encrypted data in Cloud Service Provider (CSP) to enhance the security. In the final stage, we have used the Sequential Number Generator (SNG) mechanism that drastically reduced the implemented system complexity.

Article History

Article Received: *25 March 2022*

Revised: *30 April 2022*

Accepted: *15 June 2022*

Publication: *19 August 2022*

Keywords: Cloud Computing, Data Security, Certificate Authority (CA), Attribute Based Encryption (ABE), Sequential Number Generator (SNG), and Cloud Service Provider (CSP)

1. INTRODUCTION

Cloud computing is spreading its wings, and that's why more and more organisations are relying on storing their private or confidential data on the cloud. Organisations which are storing their private data on the cloud have doubts that their data may be breached or misused by the employees of the cloud itself. Collection of documents on the cloud is suitable only if they are stored in an encrypted manner so that no one other than Cloud Service Provider (CSP) users need to be able to receive documents from cloud servers. Often, the documents need to be encrypted before being sent to the authorised user by applying any searchable encryption technique[1] to fulfil the very purpose of privacy-preserving[preserving [2].

Attribute Based Encryption (ABE) policy provide a way towards getting the correct document as a user who uses the data, he has a secret key provided by a Certificate Authority (CA). The specified document from the cloud is requested by the data user, documents are provided in encrypted form[3]. If the user has a specific secret key, then only that user can decrypt the document.

At present, research done on ABE[4] can be seen in many ways. One is KP-ABE, known as Key Policy Attribute Based Encryption [5][6] the other is CP-ABE, or cipher text attribute-based encryption schemes, [7] and the second is CP-ABHE-based Hierarchical Encryption[8].

Comparing these schemes, we sail across that CP-ABE schemes are additional stretchy and appropriate for general application. We have seen that CP-ABE is more powerful as compared to the KP-ABE mentioned by Z. Xia and J. Shuci[9][2] and CP-ABHE are providing good results as compared to CP-ABE and KP-ABE .

In CP-ABHE [8], Fu and Wang choose a random number for the attribute dispatcher; however, we have chosen a scheme that is based on a sequential number generator. However, it is a theoretical paper based on the model produced, and we have proposed that this model decreases the complexity as well as the computation power of the system. We have produced the simulation results for encryption time and decryption time which supports to our model.

1.1 Literature review or research background

Much work has been done using attribute-based encryption. In attribute based encryption [26] Data is encrypted with public attributes and decrypted with the user's private key. Keys are assigned by using Certifying Authority so that keys cannot be obtained by others. In hierarchical encryption user can encrypt the text by using her public keys and decrypted by her secret key. In Hierarchical encryption, a user which will be in the top having right to encrypt data by using her public key, at the same time, you can access the data of users located at lower levels of the hierarchy. Researchers have contributed in the algorithm based on KP-ABE and Cipher text policy attributes encryption. In Hierarchical Identity encryption provides confidentiality. CP-ABE scheme is also used in IOT based systems.

A thorough literature review is presented in the form of a table given below:

Reference No	**Methodology**	**Performance**	**Merits**	**Limitations**
[1]	Hierarchical identity based encryption (HIBE)	Provides confidentiality without sharing secret key among nodes	Using block chain, edge based IoT for collecting the data and for encrypting using HIBE	Fits suitable for event driven IoT devices
[2]	Secure data exchange between users and cloud resources is implemented using Elliptic Curve Cryptography (ECC) and session key manageme nt.	Private key sec urity by generating keys at KDC , keys are hidden to CDN and store in the key sub center	Security of the private key	Upload, encrypt, downl oad, and decrypt files aft er verifying EC C and session key manageme nt.
[3]	Symmetric encryption scheme is used for encryption, CPABE and outsourced data encryption, Java JPBC	storage cost, improved encryption and decryption time, as compare to CPABE	One common hierarchical structure is used for encrypting various messages	Ten different files of size 1 KB are taken into consideration

	Library,			
[4]	hierarchical , k-means clustering and of Expectation and Maximization technique used for cloud security ABE is used	ECC, ABE, RSA and MD5 are compared and found ABE is more suitable as compare to CP-ABE and KP-ABE is performed and establish that Cipher text attribute based encryption is better than other scheme.	CP-ABE is suitable for fine-grained access control and security.	Comparison of CP-ABE and KP-ABE
[5]	CP-ABHE scheme is used for document collection. Java Pairing Based Cryptography(JPBC) And cpabe toolkit used for simulation purposes.	CP-ABHE has been found to be superior to CP-ABE and KP-ABE.	CP-ABHE has been found to be superior to CP-ABE and KP-ABE. schemes in terms of storage space as well as encryption and decryption efficiency.	This is unfeasible for a large documents collection because the documents attribute set are random.
[6]	Encryption and decryption is performed by applying HE3 layer efficient encryption at the edge	HE3 scheme yielded better computational cost compared to OOM CP-ABE and CP-ABE.	This scheme found to be efficient in terms of encryption time, decryption time , and computational cost.	There is possibilities to work in the direction to minimize communication and storage cost.
[7]	CLR-HABE Continuous	CLR-HABE. Semantically s	CLR-HABE requires	Scheme does not deal with

	Leakage resilience(CLR)-HABE	ecure against chosen-plaintext attacks and chosen access structures	less exponentiation as levels increase	auxiliary input leakage model
[8]	Use multi-dimensional access control to approve and revoke users with multiple privileges at runtime in the cloud	Less communication overhead occurred in MDAC. Less no of elements are transmitted in both MD-AC and LCHWY schemes from cloud data provider to the server.	i) Minimize the role of the Central Authority (CA) to avoid being the primary target of ii) dynamically revoke user at any stage III) avoiding the reencrytion of ciphr text iv) Without generating the token user would not able to decrypt the text	Blacklisting a specific user Permission notarization range
[9]	Matrix used as a access structure in the (LSSS) Linear Secret-Sharing Schemes	Scheme is simpler, scalable, as compared to others	The proposed scheme is a novel CP-ABE, that is practical as well as mostly secure standard model	Focus is on black box traceability
[10]	There are mainly four different phases used in NVO-CP-ABE scheme, they can be described as Setup, key generation, data encryption,	Encryption and decryption computation improved by this scheme.	The proposed scheme improves the computational efficiency that is used for the computations to the proxy server in big data for outsource	Work required on revocation

	and data decryption.		encryption and decryption .	
[11]	This plan comprises of two module mainly tree encryption and integrated access tree development.	Theoretical examination depicts that CP-ABHE is far better and performing consistently better than both CP-ABE and KPABE	The proposed scheme found to be better as far as other scheme that is KP-ABE and CP-ABE, when we compare on the basis of efficiency and storage space and encryption time.	Theoretical examination is done
[12]	HASBE: Hierarchical Attribute Set-Based Solution in Cloud Computing.	project demonstrate that HASBE has good performance	Provides scalable, flexible, fine-grained access control	Only attribute-based encryption is considered
[13]	The platform that is used for implementing algorithms & compared using Java Integrated Development Environment(Eclipse).The inbuilt packages of java and Java crypto which are used for security.	The Performance is evaluated on different encryption scheme.	It shows that Blowfish technique obsessive less time when it is compared to different other techniques.	Each and every algorithm used has its own strength and weakness
[14]	Implements RH-CPABE based on the Java Pairing Based	Encryption is improved	Storage optimization is achieved using RH-CPABE scheme.	RHCPABE doen not optimize decryption time and it

	Cryptography (JPBC) library. Implementation is done using a 160-bit elliptic curve scheme based on a 512-bit finite hypersingular curve array .			needs to be further improved
[15]	This scheme is based on KB B trees using Vector Space Model (VSM) and UD MRS. i.e. unencrypted dynamic multi-keyword ranked search	Security analysis depict that Index and Query confidentiality can be protected in the known cipher text model by using BDMRS scheme	This scheme achieves high search efficiency	The scheme addresses the challenges of cloud servers rather than multi-user schemes.

2. MATERIALS AND METHODS

The document sharing cloud model discussed in this paper consists of mainly four entities – cloud server, data owner, data consumer, certificate authority (CA) hub.

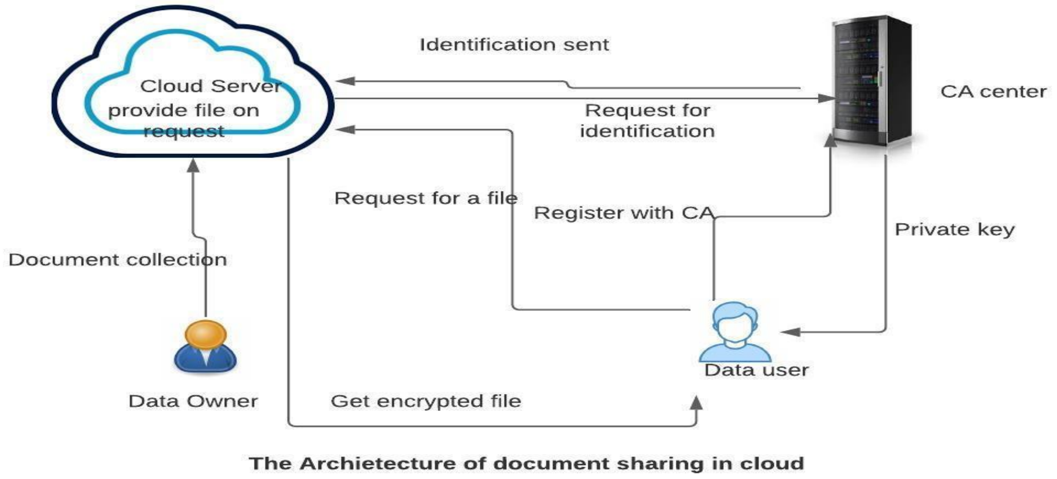

Figure1. Document Sharing Architecture used in the Cloud

The document sharing cloud model consists of mainly four entities discussed in this paper are- Cloud servers, certification authorities, data owners and data consumers, and certification authority (CA) hubs.

This section provides basic definitions and concepts related to bilinear maps.:

Definition of a Bilinear Map

Suppose we have two multiplicative cyclic groups G and G' of order k. where g is the generator of G.

Let e be a bilinear map such that

$e: G X G' \rightarrow G'$ has three properties-

(i) Bilinearity property: For r,s € G a,b € Z*

e (ra sb) = e(r.s)ab

(ii) Non-Degeneracy property: for r,s €G $e(r,s)\neq 1$

(iii) Distributive property: for r,s,t € G and a,b,c € G’

$e\ (r^{a}, s^{b}, t^{c}) = e(r^{a},s^{b})\ e\ (r^{a},t^{c})$

In addition to this, if G and e are bilinear group and bilinear map respectively then

$$G X G \rightarrow G'$$

This shows that G X G’ are efficiently computable.

There are four main algorithms, Setup, key generation, encryption and decryption based on CP-ABE. Hierarchical Encryption based on ciphertext policy attributes. A description of these algorithms is given below:

Setup: A data owner can encrypt data with a public key, and a data user can encrypt data with a private key MK generated by a central authority (CA).

Key Generation: The attributes set which is linked to the user and the master undisclosed key that is known as secret key which works as an input to the key generation. Decryption is done using the private key Sk., that is already encrypted by the use of access structure T if it matches T.

Encryption: Encryption algorithm uses a message, and an access structure for a set of attributes, along with the public key Pk. Method encrypts message with message and access structure. It produces cipher text in response to the plain text.

Decryption: Plain text can be obtained by applying the decryption process on the cipher text with the help of a specific secret key based on a set of attributes. Secret key plays an important role in the decryption process.

This entire process for data users to retrieve data from cloud servers is described below :

1. First, the data owner, which will store the documents on the cloud server, has to collect and assign an attribute key to each document. It is a two-step process. Documents are encrypted with a key and further encrypted with ABE technique, and in the end, both the document and the encrypted keys are stored on the server of cloud.
2. Data users register himself with the Certifying Authority hub to get attribute set and private key to open encrypted document issued by cloud server.
3. Query received by cloud server from data user, assuming that the cloud server is a trusted server as described by Z. Fu, K. Ren, and Z. Xia, X. Wang [1][2].
4. As soon as cloud server receives request from the server, it validate it with CA hub and gets the ID of the authorised user. If the ID is matched as received earlier by data user it confirms that a user is authorised.
5. The cloud server looks up the authorized user's query request and receives the specified document, and sends it to the data user if the attributes of the document match.
6. First, the data owner, which will store the documents on the cloud server, has to collect and assign an attribute key to each document. It is a two-step process. Documents are encrypted with a key and further encrypted with ABE technique, and in the end, both documents and encrypted keys are stored on cloud servers.
7. Data user registers with the CA hub and obtain an attribute set and a private key to open encrypted documents issued by the cloud server.
8. In this step data user send the query towards cloud server, if the cloud server is a trusted server as described by Z. Fu, K. Ren, and Z. Xia, X. Wang [1][2].

9. After receiving the request from the cloud server, validate it with the CA hub and get the canonical user ID. If the ID matches the one previously received from the data user, this confirms that the user is authorized.
10. Query from the authorised user being searched on cloud server, gets the specified document and sends it to the data user if the document's attributes match.
11. Data users decrypt documents received encrypted from cloud servers, further data user then uses his private key to decrypt the specified key to decrypt the document. The process is now complete.

Attribute based encryption scheme for document collection provides fine-grained access control. Data owner selects keys c_k sequentially from the given set of documents. The reason behind selecting the encryption key of the document sequentially is that it will reduce the computation power of the system drastically. Hence, since we are storing the data on the cloud, we have used a sequential generator rather than a random number generator so that the system will be faster as less computation power is needed. We are also proposing two levels of security at the entry level of data users. Users first login with their credentials and at the same time user should also use their biometric details to access the document from the cloud; however, the user receives the document in encrypted form. This can be further decrypted using a private key issued by a certificate authority.

In the following algorithm, we have employed a sequential number generator for accessing the documents from the cloud rather than using a random number generator, which in turn reduces the overall complexity and computation load from the cloud server’s end.

Algorithm 1: Sequential Number Generator

```
Sequence Number Generator (F, n)
F1=1, Fn=K
R=A[]      //Dynamic array
n=0
For i ← 1 to K
```

```
    if $Fi<=Fk$
    than $R \leftarrow Fi$
    End if
    $i \leftarrow i+1$
    Else "Storage is full"
If authentic=true
Retrieve documents
End if
Else not retrieve documents
Apply CP-ABE
Then generate the secret key MSK
End for
```

The above algorithm can be understood by the simple flow diagram as shown below.

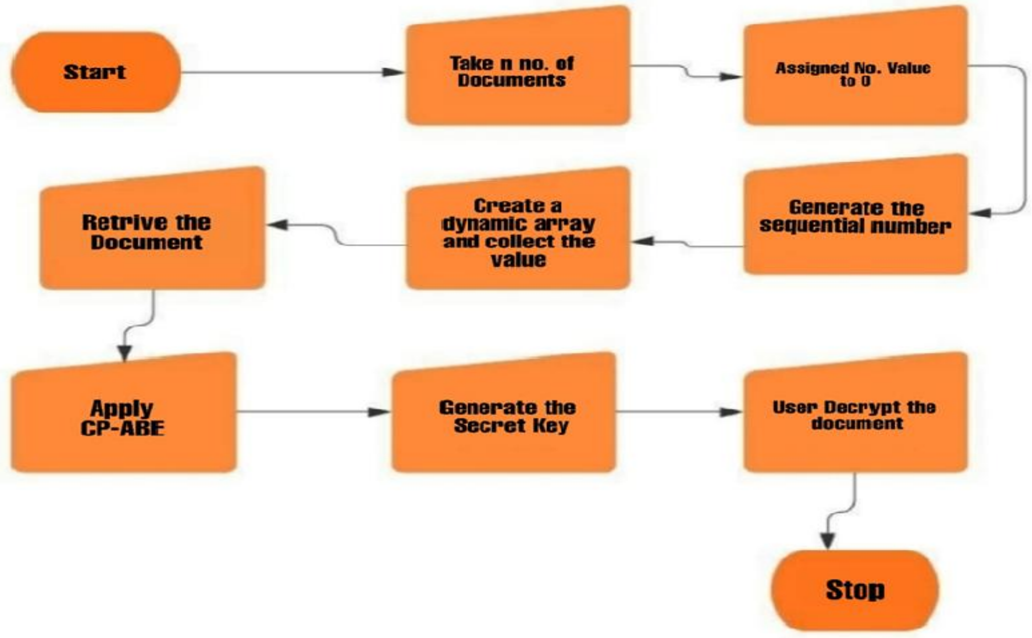

Figure 2. Flow diagram for accessing the page from the cloud server.

3. RESULTS & DISCUSSION

Java Integrated Development Environment Net Beans is used for the implementation and comparison of all the algorithms and for security algorithms are used using java packages java crypto and java security. Performance was measured with the help of Intel Core(TM) i3-8145U CPU clocked at 2.30 GHz and 4 GB RAM running Windows 10 operating system. We compared encryption times of CP-ABE, KP-ABE, and CP-ABHE using the SNG technique. We have found that the comparative result which can be better described by the figure3. As we can see in the figure, the KP-ABE and CP-ABHE using SNG results are similar to CP-ABHE and in some cases it produces better than the older scheme.

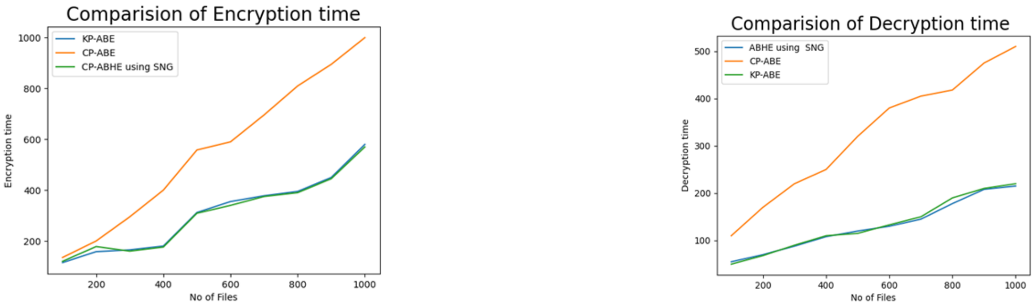

Figure3. Comparisons of Encryption time and Decryption time

4. DISCUSSION AND CONCLUSIONS

Extensive work has been done on ABE, KP-ABE, CP-ABE and CP-ABHE schemes. In all the schemes in which documents are accessed using random number generation. In this paper, we have proposed the sequential number generator (SNG) attribute dispatcher for accessing documents from the cloud rather than random numbers. By choosing sequential numbers as compared to random numbers, it will reduce the complexity as well as the computation power of the system.

Simulation results provided in the figure 3 for encryption and decryption time show the comparison of the different schemes. In the figure it has been shown that the results are better as compared to the previous scheme. In our further research work we will focus on making the better performance to enhance the scheme may be by involving fuzzy based SNG techniques.

5. REFERENCES

[1] D. Pavithran, J. N. Al-Karaki, and K. Shaalan, “Edge-Based Block chain Architecture for

Event-Driven IoT using Hierarchical Identity Based Encryption," *Inf. Process. Manag.*, vol. 58, no. 3, p. 102528, 2021, doi: 10.1016/j.ipm.2021.102528

[2] N. Soms, "An Effective Hierarchical Key Management System Using Elliptic Curve Cryptography And Session Key Establishment On Cloud," vol. 9, no. 2, pp. 263–267, 2022.

[3] T. N. Mujawar and L. B. Bhajantri, "An Attribute-Based Encryption Method Using Outsourced Decryption and Hierarchical Access Structure," pp. 75–81, 2022.

[4] P. Kanimozhi and T. A. A. Victoire, "Secure Sharing of IOT Data in Cloud Environment Using Attribute-Based Encryption," *J. Circuits, Syst. Comput.*, vol. 30, no. 6, 2021, doi: 10.1142/S0218126621501024.

[5] J. Fu and N. Wang, "A Practical Attribute-Based Document Collection Hierarchical Encryption Scheme in Cloud Computing," *IEEE Access*, vol. 7, no. c, pp. 36218–36232, 2019, doi: 10.1109/ACCESS.2019.2905346.

[6] S. Porwal and S. Mittal, "HE3: A hierarchical attribute based secure and efficient things-to-fog content sharing protocol," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1312–1325, 2022, doi: 10.1016/j.jksuci.2019.08.014.

[7] J. Li, Q. Yu, and Y. Zhang, "Hierarchical attribute based encryption with continuous leakage-resilience," *Inf. Sci. (Ny).*, vol. 484, pp. 113–134, 2019, doi: 10.1016/j.ins.2019.01.052.

[8] K. Riad, T. Huang, and L. Ke, "A dynamic and hierarchical access control for IoT in multi-authority cloud storage," *J. Netw. Comput. Appl.*, vol. 160, no. March, 2020, doi: 10.1016/j.jnca.2020.102633.

[9] H. Qiao, H. Ba, H. Zhou, Z. Wang, J. Ren, and Y. Hu, "Practical, provably secure, and black-box traceable CP-ABE for cryptographic cloud storage," *Symmetry (Basel).*, vol. 10, no. 10, pp. 1–17, 2018, doi: 10.3390/sym10100482.

[10] P. K. Premkamal, S. K. Pasupuleti, and P. J. A. Alphonse, "A new verifiable outsourced cipher text-policy attribute based encryption for big data privacy and access control in cloud," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 7, pp. 2693–2707, 2019, doi: 10.1007/s12652-018-0967-0.

[11] M. T. Scholor and A. Pradesh, "Attribute Based and Hierarchical Encryption Scheme for Documents in," vol. 13, no. 1, pp. 1585–1593, 2020.

[12] V. Mahapatra, S. Khanadagale, A. Bale, and P. P. Chandratre, "HIERARCHICAL LEVEL SECURITY IN CLOUD COMPUTING," pp. 2010–2012, 2017.

[13] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for

data security in cloud computing," *Proc. - 2017 3rd Int. Conf. Adv. Comput. Commun. Autom. (Fall), ICACCA 2017*, vol. 2018-Janua, pp. 1–7, 2018, doi: 10.1109/ICACCAF.2017.8344738.

[14] J. Shuci, G. Weibin, and F. Guisheng, "Hierarchy Attribute-Based Encryption Scheme to Support Direct Revocation in Cloud Storage," *2017 IEEE/ACIS 16th Int. Conf. Comput. Inf. Sci.*, pp. 869–874, 2017, doi: 10.1109/ICIS.2017.7960114.

[15] H. Li and T. Jing, "A Cipher text-Policy Attribute-based Encryption Scheme with Public Verification for an IoT-Fog-Cloud Architecture," *Procedia Comput. Sci.*, vol. 174, no. 2019, pp. 243–251, 2020, doi: 10.1016/j.procs.2020.06.080.

[16] L. Coppolino, S. D'Antonio, G. Mazzeo, and L. Romano, "Cloud security: Emerging threats and current solutions," *Comput. Electr. Eng.*, vol. 59, pp. 126–140, 2017, doi: 10.1016/j.compeleceng.2016.03.004.

[17] M. Abinaya and T. Sivakumar, "Secure Key Management Scheme for Dynamic Hierarchical Access Control Based on ECC," vol. 5, no. V, pp. 1076–1080, 2017.

[18] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel Classification of Security Concerns in Cloud Computing," *Appl. Comput. INFORMATICS*, 2016, doi: 10.1016/j.aci.2016.03.001.

[19] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of the IEEE Symposium on Security and Privacy (S&P), pp. 321–334 (2007)

[20] N. Soms, "An Effective Hierarchical Key Management System Using Elliptic Curve Cryptography And Session Key Establishment On Cloud," vol. 9, no. 2, pp. 263–267, 2022.

[21] H. Li and T. Jing, "A lightweight fine-grained searchable encryption scheme in fog-based healthcare iot networks," *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019, doi: 10.1155/2019/1019767.

[22] G. B. Prakash, N. Nalini, and C. Ajmeera, "EXPERIMENTS WITH ABE SCHEMES ON OPENSTACK FUEL IAAS PLATFORM," vol. 8, no. 5, pp. 647–654, 2017.

[23] S. Tang, X. Li, X. Huang, Y. Xiang, and L. Xu, "Achieving Simple, Secure and Efficient Hierarchical Access Control in Cloud Computing," *IEEE Trans. Comput.*, vol. 65, no. 7, pp. 2325–2331, 2016, doi: 10.1109/TC.2015.2479609.

[24] S. Jafarpour and A. Yousefi, "Security Risks in Cloud Computing : A Review," vol. 6, no. 4, pp. 1174–1179, 2016.

[25] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *J. Netw. Comput. Appl.*, vol. 75, pp. 200–222, 2016, doi:

10.1016/j.jnca.2016.09.002.

[26] A. Sahai and B.Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology – Euro crypt, volume 3494 of LNCS, pages 457–473. Springer, 2005.

[27] Zhang,P.,Chen,Z.,Liu,J.K.,Liang,K.,Liu,H.,2018.An efficient access control scheme without sourcing capability and attribute update for fog computing. Future Generation Computer Systems78, 753–762.

[28] Alexandros Bakas and Antonis Michalas, "Modern family: A revocable hybrid encryption scheme based on attribute-based encryption, symmetric searchable encryption and SGX", In SecureComm 2019, pages 472–486, 2019.

[29] H. Hong, Z. Sun, X. Liu, "A key-insulated CP-ABE with key exposure accountability for secure data sharing in the cloud," KSII Transactions on Internet and Information Systems, 10(5), 2394, 2016, DOI: 10.3837/tiis.2016.05.024

[30] H. E. Ga_f and A. Toumanari, \E_cient ciphertext-policy attribute-based encryption constructions with outsourced encryption and de-cryption", J. Secur. and Commun. Netw., vol. 2021, pp. 1{17, 2021(DOI: 10.1155/2021/8834616).

[31] Ruqayah R. Al-Dahhan, Qi Shi, Gyu Myoung Lee, and Kashif Kifayat. 2019. Survey on revocation in ciphertext-policy attribute-based encryption. Sensors 19, 7 (2019), 1–22.

[32] Liu,Z.,Cao,Z.,Wong,D.,2012.White-boxtraceableCiphertext-PolicyAttribute-based Encryption supporting any monotone access struc-tures. IEEE Transactions on Information Forensics and Security8,76–88.

[33] De Caro, A.; Iovino, V. jPBC: Java pairing based cryptography. In Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC 2011), Kerkyra, Greece, 28 June–1 July 2011; pp. 850–855.

[34] Doshi, N.; Jinwala, D.C. Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption. Secur. Commun. Netw. **2018**, 7, 1988–2002.

[35] Jiang, Y.; Susilo, W.; Mu, Y.; Guo, F. Flexible ciphertext-policy attribute-based encryption supporting AND-gate and threshold with short ciphertexts. Int. J. Inf. Secur. **2018**, 17, 463–475.

[36] Patil, P., Narayankar, P., Narayan, D.G., Meena, S.M., 2016. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and blowfish. Proc. Comput. Sci. 78.

[37] Porwal, S., Mittal, S., 2017. Implementation of Ciphertext Policy-Attribute Based Encryption (CP-ABE) for fine grained access control of university data. In: Tenth International Conference on Contemporary Computing (IC3). IEEE, pp. 1–7.

[38] J. Zhao, P. Zeng, and K. R. Choo, \An e_cient access control scheme with outsourcing and attribute revocation for fog-enabled e-health", *IEEE Access*, vol. 9, pp. 13789{13799, 2021 (DOI: 10.1109/ACCESS.2021.3052247).

[39] J. Li, H. Wang, Y. Zhang, J. Shen, "Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing," Ksii Transactions on Internet & Information Systems, **10**(7), 2016, DOI: 10.3837/tiis.2016.07.026.

[40] H. Takabi, J.B.D Joshi, G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, **8**(6), 24-31, 2010, DOI:10.1109/COMPSAC.2008.100.