DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



# Survey on Automatic Revocation Schemes for Cloud Systems

Manahil Awad Sherfi[1], TajElsir Hassan Suliman[2], NourEldien A. NourEldien[3]
[1]*University of Science and Technology, Sudan.*
[2]*Sudan Academy for Banking &Financial science, Sudan.*
[3]*University of Science and Technology, Sudan.*
[1]*Mnahil.awad1986@gmail.com,* [2]*tagsir@sabfs.edu.sd,* [3]*nnoureldien@acm.org*

***Abstract***— *Automatic Revocation means performing the revocation task automatically by the proxy Re-Encryption (PRE), without any command from the data owner. For the lack of survey studies that tackle the automatic Revocation Process, this paper demonstrates a rich survey on the recent auto-revocation schemes proposed by the research community. To accomplish the survey, a literature review methodology, which includes seven steps, is followed. The study concluded with the following results: clarifying the concept of automatic revocation identifying the current proposed automatic revocation schemes, classifying the proposed automatic user revocation schemes, and presenting suggestions of future research directions for revocation schemes.*

***Index Terms***— *automatic, revocation, CSP, cloud.*

## I. INTRODUCTION

To benefit from the advantages of cloud computing, data owners can take and put their data in cloud. Further they can encrypt their data to provide more security in terms of integrity and confidentiality. In case of encryption, a data owner must have means to distribute decryption keys to legitimate users. The above solution is impractical and tedious; since the data owner must be able to follow online users requesting accessing data to provide them with keys, in addition to the unreliability of communication. [6][45]

Data Owner can delegate user revocation to Cloud Service Provider (CSP), this enables CSP to revoke users without any command after initial setup. With this solution, the revocation process becomes automatic and reduces many computations from the data owner. This delegation has to implement securely and without revealing information.[9][37]

This paper is organized in six sections. In section two we list the proposed revocation schemes, in section three we demonstrate the applied methodology, in section four we discuss and compare the proposed schemes presented in the literature review. Section five concludes the paper and in section six we give sights for the future directions of automatic revocation.

*Received 27/4/2021; Accepted 25l6l2021*

 ***ISSN (Print) 1811-9212*** ***ISSN (Online) 2617-3352***

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



## II. METHODOLOGY

A methodology, which includes seven steps, is applied to conduct this study, table 1 illustrates the steps, and an explanation for each step is presented, briefly.

TABLE 1. APPLIED METHODOLOGY

| Step# | Step | Brief Description |
|---|---|---|
| 1 | Searching | Skimming related journals and scientific papers published in flagship sites such as Cloud Security Alliances, , National Institute of Science and Technology),IEEE, ACM, Google Scholar The keywords used for searching are a combination of strings such as 'security in cloud computing, data-sharing, revocation, automatic, etc. We restricted the search process for articles published in between 2005-2020. |
| 2 | Obtaining | The download papers relevant to our search keywords are stored in dedicated folders. |
| 3 | Assessing | After obtaining and storing articles, we make a quick skim to determine whether the article is closely relevant to our topic or not. We first read the abstract, introduction, and first few paragraphs, and the conclusion of each article, we attempted to find out the research problem, applied methodology, the contribution of the paper. If we find that article is focused on |

Received 27/4/2021; Accepted 25l6l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



| | | |
|---|---|---|
| | | automatic revocation in cloud computing, then the article is considered relevant. |
| 4 | Reading | Once we find the paper is within our study scope, we proceed further to read the rest of the paper, This precise reading provides us with an excellent overview about the research community effort to solve the corresponding problem, moreover, their contribution and added knowledge are investigated. |
| 5 | Critical Evaluation | The evaluation of the paper relevancy we done again based on the entire content of the assessed literature. Articles that provide unrepeated, original information about fine-grained access control are considered relevant. The relevant articles are grouped based on the exact topic the papers cover. |
| 6 | Recording/ Summary | In this step, we summarized the reviewed papers and sum up the contents, mainly focused on the papers published during the period 2005-2020. Some important encryption schemes, and the way they implement these schemes to provide the automatic revocation. All reviewed papers are cited using https://scholar.google.se/ |

*Received 27/4/2021; Accepted 25l6l2021*

 **ISSN (Print) 1811-9212** **ISSN (Online) 2617-3352**

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



| | | |
|---|---|---|
| 7 | Writing Critical Review | Based on the obtained articles published in the years 2005-2020 and the summaries we made, we write the literature review sections, using technical tips in writing a literature survey.<br>Based on collected automatic revocation schemes, we provide classification to the proposed schemes. |

## III. AUTOMATIC REVOCATION SCHEMES

The automation of revocation comes from the manner the CSP implements the re-encryption process and the underlined encryption algorithm. Two categories of Auto-Revocation solutions have been proposed: Time-based solutions [1],[2],[3], and Task-based solutions [4].

### A. Time-based Schemes

In this section, we discuss what is called time-based revocation schemes. In these schemes the user's access rights and privileges are expired automatically after a predefined period of time is expired.
A time-based re-encryption scheme called (R3) that provides the cloud servers with the ability to re-encrypt the data in an automatic manner based on their internal clocks is proposed in [1]. This proposed scheme is developed on top of ABE, to permit fine-grain access control, without seamless clock synchronization for accuracy.

The basic idea behind the above method is to combine both time and access privileges as a data feature. To access data, each user has to own keys that have access to specific data attributes and have a time validity. Users can decrypt data using their keys that match data attributes and access time.

A scheme that based on a clock proxy and on the CP_ABE scheme is proposed in [2]. The proposed scheme is called a clock-based proxy re-encryption (C-PRE) scheme or (TimePRE), and it works by segmenting Time into segments frames that form a tree. The height of this tree can be changed as needed. For simplicity, the authors segment the Time tree into three layers, year, month, and day. As shown in *Fig.* 1.

The scheme (TimePRE) allows the data owners and the cloud service provider to exchange secret keys in advance. This allows cloud providers to compute the PRE keys using their internal clock, and use these keys later to encrypt cypher text.

Received 27/4/2021; Accepted 25l6l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



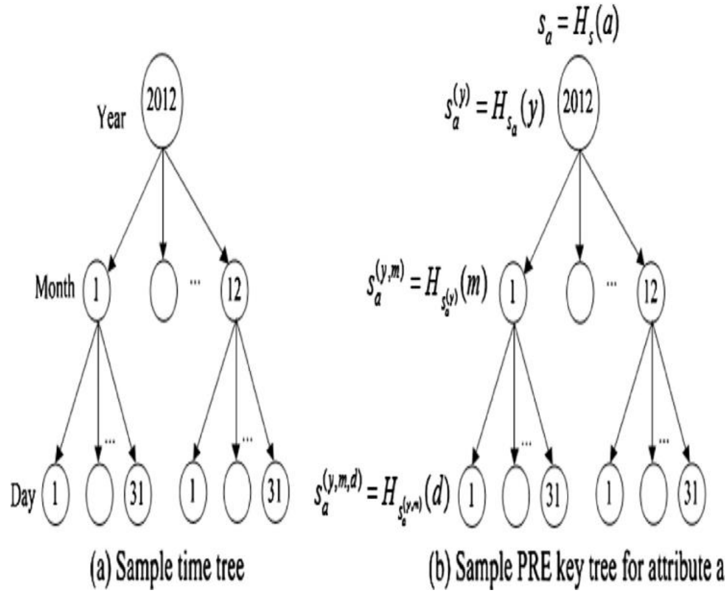


FIG. 1. TIME PRE KEY TREE

In [3] authors proposed an enhanced scheme called (HASBE) which is flexible and provides grained access control in supporting multiple attributes of ASBE. In addition, HASBE employs compound value assignments for access expiration time to deal with user revocation more efficiently than the above counterparts.

To illustrate the mechanism of the HASBE scheme, let us consider a hierarchical cloud environment shown in *Fig*. 2, where the cloud service provider manages a cloud to provide data storage service. Data owners encrypt and store their data in the cloud for sharing with data users. Data users download preferably encrypted data from the cloud and decrypt them. Each data owner/consumer is controlled by domain authority. Domain authority is managed by its confidential authority.

HASBE is classified as the enhanced version of ASBE in automatic user revocation. The scheme adds a new element called (expiration_time) to a user's key, to determine the lifetime of the key. Then the policy associated with data files can check the expiration_time element as a numerical comparison.

For a better understanding of HASBE mechanism, assume a data owner (o) has a key with expiration_time (k) and a data file whose access policy is associated with expiration_time (f), hence (o) can decipher this data file only when $k \geq f$ and the rest of the policy matches attributes. In a real implementation, the required time for accessing the precious elements has to be very small to reduce the vulnerabilities when the encryption key is exposed at any time.

Received 27/4/2021; Accepted 25l6l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



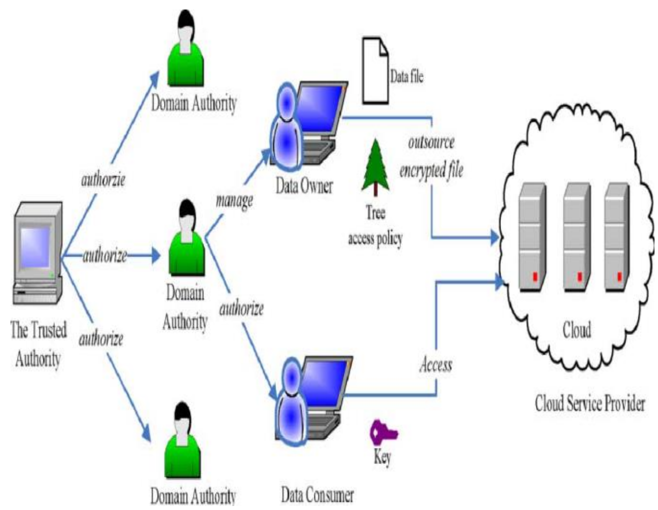


FIG. 2. HIERARCHICAL CLOUD ENVIRONMENT

## B. Task-based Schemes

The limitation of accessing the cloud data to a certain and predefined time slot is impractical since the access is expired before the task is carried out or done, hence the time-based schemes experience the above weakness and limitation. The alternate approach is a task-based revocation scheme.

In the following sections, we presented a promising scheme that applied the new task-based concept.

In [4] Mahmood Ahmad etal. proposed a system that allows authorized users to access encrypted data for predefined attempts rather than pre-defined time.

In the aforementioned scheme, the user is authorized for a limited number of access to the data. Hence, the granted portion is free from time constraints. Processing the user request is explained below.

The model has to get $\alpha_i$ to generate P (.) for the accessing user, and the of $\lambda i$ is generated by getting $\lambda i$ and $\lambda i + \alpha i$ *as parameters*. A constant $C$ *is generated from* $P(.)$ and is split into $c_1$ and $c_2$, where $C = c_1 + c_2$. A single user identifier Ʊi $\epsilon$ N is generated and will be used to authenticate the user. The user is granted the deciphering key $k$ and Ʊ. A maximum number from $P(.)$, $c_1$,$\lambda_i$, and Ʊ are set to TTP besides $\sigma_{pk}$ and $\sigma_{sk}$. The cloud service provider with $EH(c_2, \sigma_{sk})$, is given the minimum number from $P(.)$ ciphered using $\sigma_{sk}$ and $\sigma_{pk}$. After this scattering takes place, the user gets benefits from the available services whenever he wants. Table (2) illustrates the hypotheses and symbols used to depict the above scheme.

Received 27/4/2021; Accepted 25l6l2021

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

Iraqi Journal of Computers, Communications, Control & Systems Engineering (IJCCCE), Vol. 21, No. 3, Sep 2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5 

TABLE 2. HYPOTHESES AND SYMBOLS USED IN [4]

| **Notations** | **Description** |
|---|---|
| *F* | Data Owner file |
| *Ai* | User number of attempts to access *F* |
| *P*(.) | A predetermined degree Polynomial generated for the legitimate user |
| *Λi* | Offset value for a user |
| Θ | Lowest degree factor in *P* (.) |
| *C* A | The fixed number took from *P*(.) |
| Λ | No of encrypted values calculated with TTP |
| Δ | Ignorant-Value computed by CSP for any user appeal |
| *Es*, *Ds* | Secret key ciphering and deciphering algorithms |
| *EH*, *DH* | Homomorphic ciphering/ deciphering algorithms |
| *σpk*, *σsk* | A couple of keys for Homomorphic ciphering |
| *k* | the private key of the conventional algorithm |

The assessment of user's appeal and withdrawal of user endorsement through echo effect will be discussed below:

For the appeal seeming the first time, TTP takes $\lambda$ and cipher it using $\sigma sk$ i.e., $\varepsilon H(\lambda, \sigma_{sk}) = \lambda\sigma_{sk}$ . Likewise, TTP computes $\varepsilon H(\lambda_2 + c_1, \sigma_{sk}) = \lambda_2 + c_1\sigma_{sk}$ and hand these encoded values to a cloud service provider. Λ Equation 1 represents the encrypted values:

$$\Lambda = \lambda_2 + c_1\sigma_{sk} \quad \ldots\ldots(1)$$

Received 27/4/2021; Accepted 25l6l2021

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5

Upon receiving of $\Lambda$ from TTP, CSP computes ($\Theta \oplus \sigma_{pk}\ c\sigma_{sk2}$ ) and ($\lambda\sigma_{sk} \oplus \sigma_{pk}\ \lambda\sigma_{sk}$ ), where $\oplus\ \sigma_{pk}$ stands for the homomorphic multiplication given $\sigma_{pk}$. Value of $\Theta$, c $\sigma_{pk\ 2}$, and σpk are pre-setting to cloud service provider when the system is set up with σpk, CSP performs the homomorphic process $\oplus\sigma_{pk}$ on these parameters to get an ultimate ignorant vector Δ(see equation 2).

$$\Delta = \Lambda \oplus \sigma pk\ (\Theta \otimes \sigma pk\ c\sigma sk\ 2\ ) \oplus \sigma pk\ (\lambda\sigma sk \otimes \sigma pk\ \lambda\sigma sk) \quad \ldots\ldots..(2)$$

The reply of appeal is directed to data consumers via TTP since Δ is shared with TTP only. In receipt of Δ, TTP deciphers it with $\sigma_{sk}$ *and shown in e*quation 3:

$$DH(\Delta, \sigma_{sk}) = \Phi_x \ldots\ldots (3)$$

$\Phi_x$ ={ $\Phi echo$ *= First and last request only* **or**

$$\Phi_{residual} = \text{first and last appeals are excluded} \ldots\ldots \quad (4)$$

For the user, appeal seeming arrives first. TTP saves the result obtained from equation 3 as $\Phi_{echo}$. For all following appeals, the value returned as $\Phi_x$ is contrasted with $\Phi_{echo}$.Φ is equal to $\Phi_x$ only when the user is stick to the legal number of tries. Up to this equivalence is takes place, the TTP will return $\Phi_x$ as $\Phi_{residual}$, where $\Phi_{residual}$ is a nonce giving no evidence when $\Phi_{echo}$ *raises up again*. The suggested method attains appropriate results to limit user attempts and assisted in the termination of the user accessibility in an automatic manner.

## IV. DISCUSION

As we explained in previous sections of this paper, there are many schemes to automate the revocation of users, some are time-based and others are task-based. Here we'll discuss these schemes from different points of view.

Some features of time-based schemes are organized in a table (3).

TABLE 3. TIME-BASED SCHEMES

| | R3 | TIMEPRE | HASBE |
|---|---|---|---|
| Encryption Scheme | HABE | HABE | ASBE |
| Decryption Key associated with | Attribute and effective time | Attribute and effective time | Attribute and expiration time |
| # of keys/ user depend on | Length of time slice | The layer in which the user possesses its keys * | The difference between X and Y ** |

*Received 27/4/2021; Accepted 25l6l2021*

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5


One of the key factors concerned in designing R3 scheme is that combining a different ciphertext for every time slice will involve users dealing with a lot of keys. The total number of keys of R3 is related to the actual length of the time slice. This length can be set depending on the application requirements. Thus, an application that assumes to revoke users on a monthly basis will have a longer time slice, and hence has a smaller number of keys in contrast with an application where membership changes frequently (i.e. each hour).

*TimePRE* scheme cannot be directly applied with applications that require different attributes with different effective time slots.

In[1] Qin Liu et al. attempted to resolve the problem experienced by TimePRE scheme, by obliging the data owner to generate additional UAKs for every user in the GenKey algorithm., more details and examples are cited in [1].

In [2] Bobba et al. developed HASBE as extended of *ASBE* with a hierarchical structure uses a delegation algorithm similar to the one described in the CP-ABE, in addition, HASBE employs multiple value assignments for access expiration_time to deal with user revocation more efficiently than the above schemes. For example, assume a user (u) has a key with expiration_time (X) and a data file whose access policy is associated with expiration_time (Y), then (u) can decrypt this data file only when( $X \geq Y$) and the rest of the policy matches attributes. In a real implementation, the time for accessing the precious elements has to be very small to reduce the vulnerabilities when the encryption key is exposed at any time.

For automatic revocation over cloud data, access can be bounded within a certain anticipated time limit, so that the access expires beyond the effective time period as mentioned above. This time-oriented approach is more rigid and not a one-size-fits-all solution. In certain circumstances, exact time anticipation is not an easy choice. Instead, the alternate solution could be task-oriented to restrict users beyond a certain number of permissible attempts to access the data [5].

In task-oriented, user permission will remain active for a predefined number of access attempts for which permission is granted. With these insights, a task-oriented access model has been proposed in which access expires when the user has utilized his effective’s permission (i.e. no of times a user can access the allowed resources which are independent of time restrictions). Using homomorphic encryption in the evaluation of the user’s request, capable of getting good results in hiding user access limit on uploaded data on clouds, and also helps to revoke user access automatically without information revealing.

## V. CONCLUSION

In this paper, a rich survey on automatic revocation schemes is presented.
The survey found out that, most of these schemes rely on encryption algorithm called (ABE) and it is variants.
Furthermore, the survey concluded that the derived methods are classified as time-based. Moreover, the study presented a new approach namely task-based in which the resource access expires when the user has utilized his effective’s permission. For future work, we suggest developing a hybrid scheme combining time and task to efficiently control user access privileges.

*Received 27/4/2021; Accepted 25l6l2021*

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5

## VI. FUTURE RESERCH WORK DIRECTIONS FOR AUTOMATIC REVOCATION

The research in user revocation is a very promising research area. A Future research in developing new revocation schemes can take the following directions:

- Addressing inefficient revocation experienced by the time-based approach.
- Reducing high communications and computation costs (encryption, decryption, key generation operations).
- Developing new schemes that use non-monotonic access structures.
- Using of dynamic attributes to develop hybrid schemes (time, task, location,...etc.) for efficient and flexible revocation.

## REFERENCES

[1] Liu, Qin, et al. "Reliable re-encryption in unreliable clouds." *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011.

**[2]** Liu, Qin, Guojun Wang, and Jie Wu. "Clock-based proxy re-encryption scheme in unreliable clouds." *2012 41st International Conference on Parallel Processing Workshops*. IEEE, 2012.

[3] Wan, Zhiguo, Jun'E. Liu, and Robert H. Deng. "HASBE: A Hierarchical Attribute-based Solution for Flexible and Scalable Access Control in Cloud Computing."IEEE transactions on information forensics and security 7.2 (2012): 743-754.

[4] Liu, Qin, Guojun Wang, and Jie Wu. "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment." *Information Sciences* 258 (2014): 355-370.

[5] Ahmad, Mahmood, et al. "Task-oriented access model for secure data sharing over the cloud." Proceedings of the 9th International Conference on Ubiquitous Information Management and Communication. ACM, 2015.

[6] Ruqayah R. Al-Dahhan , Qi Shi , Gyu Myoung Lee, and Kashif Kifayat, "Survey on Revocation in Ciphertext -Policy Attribute-Based Encryption",
In Licensee MDPI, Basel, Switzerland,2019,

[7] Ling, J.; Weng, A. "A scheme of hidden structure attribute-based encryption with multiple authorities". In IOP Conference Series: Materials Science and Engineering; IOP Publishing: Bristol, UK, 2018; Volume 359, p.012005.

[8] Li, X.; Tang, S.; Xu, L.; Wang, H.; Chen, J. "Two-factor data access control with efficient revocation for multi-authority cloud storage systems". IEEE Access 2017, 5, 393–405.

[9] Chen, G., Xu, Z., Jiang, H. et al. "Generic user revocation systems for attribute-based encryption in cloud storage". Frontiers Inf Technol Electronic Eng 19, 1362–1384 (2018) doi:10.1631/FITEE.1800405

[10] N.Sunanda , N.Sriyuktha , P.Sai Sankar , "Revocable Identity - Based Encryption For Secure Data Storage In Cloud", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-7 May, 2019

[11] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Vol. 1. IEEE, 2012.

[12] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[13] Subashini, Subashini, and Veeraruna Kavitha. "A Survey on Security Issues in Service Delivery Models of Cloud Computing." Journal of network and computer applications 34.1 (2011): 1-11.

[14] IDC. (2009, 24 October 2012). Cloud User Surveys. Available:http://www.slideshare.net/JorFigOr/cloud-computing-2010-an-idc-update

*Received 27/4/2021; Accepted 25l6l2021*

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5

[15] Info-Tech Forum, "http://www.levelcloud.net/",last visited 27,may,2021.

[16] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," Security & Privacy, IEEE, vol. 9, pp. 50-57, 2011.

[17] S. Sundareswaran, A. Squicciarini, and L. Dan, "Ensuring Distributed Accountability for Data Sharing in the Cloud," Dependable and Secure Computing, IEEE Transactions on, vol. 9, pp. 556-568, 2012.

[18] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in MIPRO, 2010 Proceedings of the 33rd International Convention, 2010, pp. 344-349.

[19] T. Dillon, W. Chen, and E. Chang, "Cloud Computing: Issues and Challenges," in Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, 2010, pp. 27-33.

[20] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security?" University of California, Berkeley Report No. UCB/EECS-2010-5 January, vol. 20, pp. 2010-5, 2010.

[21] Sadeghi, Ahmad-Reza, Thomas Schneider, and Marcel Winandy. "Token-based cloud computing." International Conference on Trust and Trustworthy Computing. Springer Berlin Heidelberg, 2010.

[22] Security Guidance for Critical Areas of Focus in Cloud Computing, April 2009. DOI = http://www.cloudsecurityalliance.org/topthreats/csathreats. v1.0.pdf

[23] Lee, C.-C.; Chung, P.-S.; Hwang, M.-S. " A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments", IJ Netw. Secur. **2013**, 15, 231–240.

[24] Fowler Jr, Floyd J. Survey research methods. Sage publications, 2013.

[25]https://www.ischool.utexas.edu/palmquis/courses/survey.html.

[26] Wright, Kevin B. "Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services." , https://academic.oup.com/jcmc/article/10/3/JCMC1034/4614509, last visited 28, May, 2021.

[27] Zhong, H.; Zhu, W.; Xu, Y.; Cui, J.," Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage", Soft Comput. **2018**, 22, 243–251.

[28] Li, Y., Zhu, J., Wang, X., Chai, Y., Shao, S. "Optimized ciphertext-policy attribute-based encryption with efficient revocation", Int. J. Secur. Its Appl. **2013**, 7, 385–394.

[29] Horváth, M. "Attribute-based encryption optimized for cloud computing" In SOFSEM 2015: Theory and Practice of Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; pp. 566–577.

[30] Wang, Guojun, Qin Liu, and Jie Wu. "Hierarchical Attribute-based Encryption for Fine-grained Access Control in Cloud Storage Services." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.

[31] Lewko, Allison, and Brent Waters. "Decentralizing attribute-based encryption."Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, 2011.

[32] Ostrovsky, Rafail, Amit Sahai, and Brent Waters. "Attribute-based encryption with non-monotonic access structures." Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007.

[33] Yu, Shucheng, et al. "Achieving secure, scalable, and fine-grained data access control in cloud computing." Infocom, 2010 proceedings IEEE. Ieee, 2010.

[34] Bhavya.G, Parvathy Ramachandran, Manasa.V and Srividhya V.R "TIME BASED RE-ENCRYPTION IN UNRELIABLE CLOUDS", 2012 International Conference on Advances in Computer and Electrical Engineering (ICACEE') Nov. 17-18, 2012 Manila (Philippines).

*Received 27/4/2021; Accepted 25l6l2021*

DOI: https://doi.org/10.33103/uot.ijccce.21.3.5



[35] Mete, V.I.; Gothawal, M.D.B." Cipher text policy Attribute Based Encryption for Secure Data Retrieval in DTNs", Int. J. Eng. Technol. **2016**, 3, 1740–1745. [36] Zhong, H.; Zhu, W.; Xu, Y.; Cui, J,"Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage", Soft Comput. **2018**, 22, 243–251.

[37] Irfan, Mahroosh, et al. "A Critical Review of Security Threats in Cloud Computing." Computational and Business Intelligence (ISCBI), 2015 3rd International Symposium on. IEEE, 2015.

[38] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on. Vol. 1. IEEE, 2012.

[39] Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[40] P.S.V. Sainadh, U.Satish Kumar and S.Haritha Reddy, "Security Issues in Cloud Computing", International Journal for Modern Trends in Science and Technology, Vol. 03, Special Issue 01, 2017, pp. 125-130

[41] Ms. Gauri R. Thorat PG ,"A Novel Approach for Efficient User Revocation with Maintaining Shared Data Authenticity on Cloud" in International Journal on Recent and Innovation Trends in Computing and Communication, June 2015 , vol. 3 , pp. 4085-4089 .

[42] Tariqul Islam, A Classification and Characterization of Security Threats in Cloud Computing, page:14, March 2016.

[43] T. Vaikunth Pai & Dr. P. S. Aithal, "A Review on Security Issues and Challenges in Cloud Computing Model of Resource Management", International Journal of Engineering Research and Modern Education, Volume 2, Issue 1, Page Number 65-70, 2017

[44] Al-Dahhan, Ruqayah R et al. "Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption.", *Sensors (Basel, Switzerland)* vol. 19,7 1695. 9 Apr. 2019, doi:10.3390/s19071695.

[45] Sumathi, M., Sangeetha, S. "A group-key-based sensitive attribute protection in cloud storage using modified random Fibonacci cryptography", Complex Intell. Syst. (2020), https://doi.org/10.1007/s40747-020-00162-3

*Received 27/4/2021; Accepted 25l6l2021*