Received: August 23, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

IDOCA and ODOCA - Enhanced Technique for Secured Cloud Data Storage

Boopathy Duraisamy[1]* Sundaresan Muthukrishnan[1]

[1]*Department of Information Technology, Bharathiar University, Coimbatore, Tamilnadu, India.*
* Corresponding author's Email: ndboopathy@gmail.com

Abstract: Cloud storage is widely used today by many users. The cloud storage allows its users to store and access their data anytime, anywhere on demand. The cloud servers are widely spread over in different geographical locations to prevent its users from service failure and downtime issues. The cloud security prevention has been done in many ways that include making the special rules, regulations, policies and data security-related standards for cloud service providers by many countries. The Secured Cloud Data Storage Prototype Model is proposed to provide the end to end security to protect the user data from the security related issues. In this research paper, one of the SCDSPM's modules named Automatic Cloud Data Backup Model is proposed and discussed with results and comparisons. While comparing the features of the existing data backup methods the ACDBM uses two different data handling methods to store and retrieve the data from cloud storage; they are Inside Data Ownership Country Access and Outside Data Ownership Country Access. The results and performances of SCDSPM's ACDBM have effectively met the demands of the evaluation parameters as per the proposed ACDBM in testing scenario phase.

Keywords: Cloud computing, Cloud storage, Cloud data security, Data privacy, Data backup mechanism.

1. Introduction

The cloud computing has been a popular practice of using a network of remote servers hosted on the internet to process, store and manage data rather than on a local server or personal computer [1]. The cloud computing models are divided into two types. They are "cloud deployment model" and "cloud service model". Cloud deployment model includes public cloud, private cloud, hybrid cloud and community cloud. Cloud service model includes Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The computing resources and data storages [2, 3] are pooled together to provide and to maintain the user's requirements in the on-demand elasticity measures. Most of the SaaS providers are tied up with IaaS providers to store and handle [4, 5] the user's data. Moreover, most of the IaaS Providers will act as third party service providers to cloud users but users do not know about the third party IaaS provider's involvement in their cloud service.

The trust and privacy issues will be solved only by maintaining the transparency in the Service Level Agreement (SLA) [6], by providing the geographical location information of where the data are stored [7] and the third parties IaaS provider's involvement [8] in user data. Many countries like Switzerland and Australia stipulate some special regulations and standards for cloud data handling methods within their country level [9]. These countries do not allow the trans-border data flow [10] of sensitive data.

But, many countries are still in the beginning stage of cloud standardization process. Most of the countries are unable to control their countries data issues, so some of the countries are maintaining the neutral manner. The data-related issues are needed to address correctly with solutions and that will avoid and solve the data-related issues in cloud computing. The proposed Automatic Cloud Data Backup Model (ACDBM) will support the users to avoid some data-related issues in the cloud storage. The ACDBM is one of the sub-models of Secured

Cloud Data Storage Prototype Model (SCDSPM) [11, 12].

The existing backup method does not allow the users to store their data in the cloud storage as per user's data accessing and storing country.

But in the proposed ACDBM method the user will be able to store their data in two different types using data handling permission methods. The users have full rights on his/her data in IDOCA method, i.e. the users can create, modify and delete the data. But in ODOCA method the users have only limited rights on his/her data, i.e. the users can create the new data but they are not allowed to do any modification and deletion in the existing data of the cloud storage. But the users are permitted to store their modified file with modifying date and version numbering information in the proposed ACDBM method.

The features of the proposed ACDBM methods are,

- From the Outside Data Ownership Country Access (ODOCA), the users cannot delete the file in cloud storage and also cannot save the modifications in the original file in the cloud storage. It will automatically prevent the unauthorized data modifications from the outside data ownership country access.
- By using the ACDBM's two different data handling methods, the Cloud Service Providers can create trust for them. If any unauthorized modifications are done within the country limit, then that incident will be carried out within the country jurisdiction itself.

The remaining part of the paper is organized as follows: Section 2 reviews the related works concerning the ways to improve the data storage security related requirements. Section 3 describes the review of the problem statement in cloud data storage security. Section 4 explains the proposed SCDSPM's methodology. Section 5 deliberates the ACDBM algorithm for data storage and data retrieval in IDOCA and ODOCA method. Section 6 represents the implementation, experimental results and the features of the proposed method are also discussed here. Section 7 presents the conclusion of the proposed algorithm.

2. Review of literature

Cloud backup is one type of backup where the data are backed up to a storage server or facility connected to the source via internet [13]. One of the advantages of cloud backup is that the data are replicated in many places and it is offsite backup [14], so it offers protection from natural disasters. The disadvantages of cloud backup are more expensive when compared to local backup and also it will take a long time to backup or restore [15] the data. However, the online backup [16], offsite backup [17] and remote backup are nearly as time consuming as the cloud backup [18, 19].

When compared to all the backup methods, the issues related to backup methods show that the cloud storage requires more control to secure the data. Furthermore the backup mechanisms are not in the control of local jurisdictions. Hence these legal issues lead to the security-related issues in the cloud storage.

3. Statement of the problem

The security issues are rising due to the contractions and conflicts between the various countries' different data protection act which allows the CSPs to freely move on the user's data. The cloud users need to trust CSP only, based on their SLA information. The data locations of geographical positions are to be clarified at the time of SLA signing itself. The CSPs are the providers who are providing the same level of services all around the world with different data handling methods, due to the local jurisdiction and local government authority's regulations.

The CSP mostly acts with different SLA models due to the regulation conflicts between the different countries. The regulations and standards are needed to maintain at the same level by all the countries, only then it will put an end to the cloud privacy and trust-related issues.

Most of the countries are not seriously taking the trans-border data flow as serious issues due to lack of awareness of the future issues. To bring all the required things together in a short span of time is also not possible due to involvement of many countries.

So the national security policy of each country is needed to be redesigned and to reconstruct the country-level regulations in time to time interval basis. If the national policy is more than enough to control the cloud data flow before the trans-border issues, the data protection will come under the national regulatory authority control. Once the data have been controlled before the trans-border data flow, it will automatically avoid most of security and privacy-threat related issues.

To resolve this invisible problem the data backup within the user's country is mandatory to maintain the user's security and privacy. So the ACDBM proposed the mid-level solution to this CSP's trans-border data- flow-related problems.

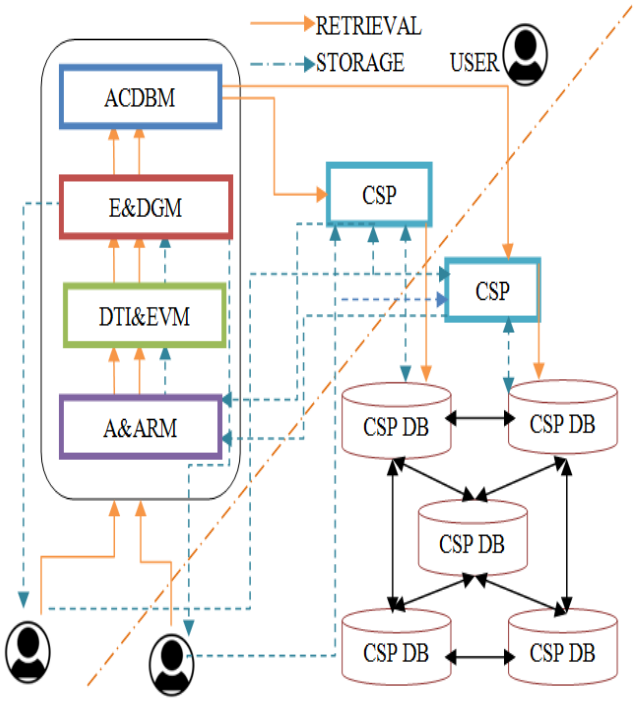

Figure.1 SCDSPM Working Structure Framework

4. Secured Cloud Data Storage Prototype Model

Secured Cloud Data Storage Prototype Model is designed to overcome some of the cloud security related issues and privacy threats, which are being faced by the users in the cloud storage. The cloud users are unaware of their data risks in cloud storage. It will raise the issues to the cloud data owners too. To reduce and prevent the user's data from such issues the SCDSPM's ACDBM is proposed.

The Fig. 1 shows the SCDSPM and its four sub-models. The sub-models of SCDSPM are: Authentication and Authorization Resolving Model, Data Type Identification and Extension Validation Model, Encryption and Decryption Gateway Model and the Automatic Cloud Data Backup Model. This research paper deals with the proposed Automatic Cloud Data Backup Model.

5. Automatic cloud data backup model

The ACDBM has been designed to back up the data automatically from the user at the time of data transferring into CSP's server.

The ACDBM server is always on idle mode and it will become active only at the time of new data being transferred to CSP's server or any modified data being transferred to the CSP's server. The ACDBM process is based on the SCDSPM's previous sub-models.

Once the ACDBM receives storage request from the user, the ACDBM first verifies the request raising user's permission and data controlling rights. If the user is accessing the data from the inside data ownership country, then that user comes under the Inside Data Ownership Country Access i.e. IDOCA mode. In IDOCA the user has rights to access the data with full permission.

If the user accesses the data from outside the country then the ACDBM allows the user to handle the data with limited control under Outside Data Ownership Country Access i.e. ODOCA mode. It means the modification on existing data will not take effect on the original data file which has already been stored in cloud server. Each and every time the modified file will be saved as file version format with the data modified date.

For example the actual file name is **jersy.doc** means, the modified file will be saving as **20-12-2015_V1_jersy.doc.** The ACDBM is storing the data in two different modes. They are Inside Data Ownership Country Access (IDOCA) and Outside Data Ownership Country Access (ODOCA).

5.1 Inside data ownership country access

In IDOCA mode, user's authorization has authorized using the user's data accessing country IP address and based on that, the IDOCA provides full permission on the data. If the user is accessing the data from data ownership country, the user is allowed to create, modify, manipulate, share and delete the data in cloud storage.

The data handling restrictions are not lifted because the data user is accessing the data within the data ownership country itself. So the data accessing risks are bound within the country limited data handling regulations and standards. Generally, if the user is accessing the cloud data using the VPN means, access request will be blocked by using the blacklisted VPN port details. The user's IP address is verified using the country IP address verification details. If the user's IP address is unable to be traced, it will automatically deny that user's request (These things should be taken care by the SCDSPM's AARM model). In IDOCA the actual file will be replaced by the new file in the ACDBM and CSP's server.

The Fig. 2 shows the data storage method in ACDBM in IDOCA mode. **N.E** will be then remaining as **N.E** while the user is storing the data in IDOCA mode. **N** defines name of the filename and **E** defines extension of that filename.

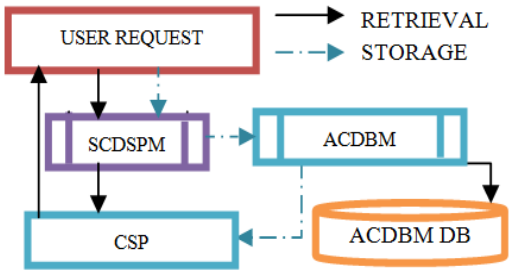

Figure.2 ACDBM in IDOCA mode

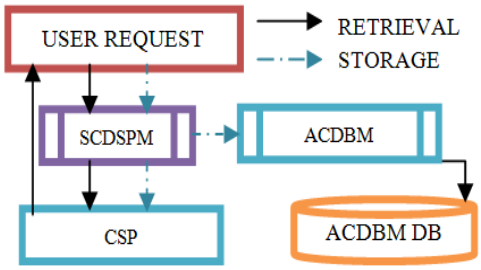

Figure.3 ACDBM in ODOCA mode

5.2 Outside data ownership country access

The ODOCA mode denotes that the user is accessing the cloud data from outside the data ownership country limit. So the ACDBM allocates only limited permission to the user. In the ODOCA mode, by default it will not allow the user to replace the existing data file in the ACDBM and CSP server. Instead of replacing the existing file, it will fix the date and file version value as a prefix value before the modified file name. Each time the user modifies the data file, these processes automatically assign the date and version value as a prefix value before the modified file name. So this process will help the user to identify the data-modification-related information based on the prefix value (i.e. date and file version value). The Fig. 3 shows the data storage method in ACDBM in ODOCA mode.

The method used to store data in ODOCA mode

$Date^{1}$_$Date^{N-1}$+_+ Version_$Number^{1}$..... ...Version_$Numer^{N-1}$ + _ + Filename. Extension.

5.3 ACDBM framework

The data transferring concept also differs in two modes. In IDOCA Fig. 2, first the data will be transferred into SCDSPM's ACDBM server and then the data from ACDBM server will be transferred to the CSP's Server. But in the ODOCA Fig. 3, the data simultaneously transferred from user system to SCDSPM's ACDBM server and CSP's server, it will help to avoid the unauthorized access to the SCDSPM server. Fig. 4 shows the framework model of Automatic Cloud Data Backup model.

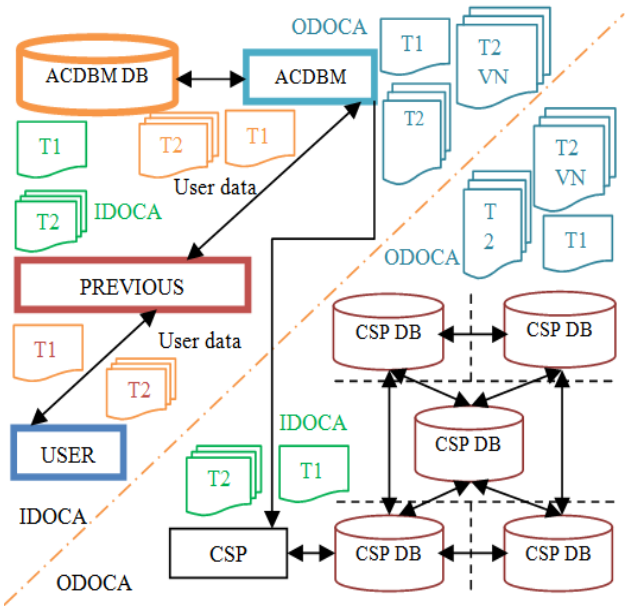

Figure.4 Framework of automatic cloud data backup model

5.4 ACDBM pseudo code

Get the request from the user to store the file
Verify the data request
If request is for new data storage **Then**
Move the data to the ACDBM and then forward that data to CSP
Else
Move the data storage request to the data handling permission verifier
If Data storage request user has **IDOCA Then**
Update the information on original data file and transfer that data to ACDBM Server and from the ACDBM Server to CSP Server
Else
Declare the Data storage request user has **ODOCA**
Store the updated information with new version of existing data file name in the ACDBM Server and CSP Server concurrently

Process in Verifying of Permission based on IDOCA and ODOCA:

Get the IP address from the ***IP address validation*** process module
Identify the IP address
If IP address is within IDOCA **Then**
Assign and Declare the full permission on file which includes Create, Modify, Replicate, Copy, Cut, Paste, Save, Save as and Delete.
Else

Assign and Declare it as ODOCA and assign the limited permission on file which includes Create, Modify, Replicate, Copy, Cut, Paste, Save as and excludes Save and Delete permissions.

6 Results and discussion

The Java 1.8 SDK version was used to design the ACDBM algorithm, and also the same java version was used to verify the efficiency and other related parameters of ACDBM algorithm. The time taken for data storage using different file types in IDOCA and ODOCA modes were compared. The resource utilization and time taken to execute the IDOCA and ODOCA modes were also calculated and compared. The time taken to upload the data file from user end to the server end and the server response time taken from the server end to the user end were not considered here, because time taken to upload the data file and result responses are based on the bandwidth speed of the user. Also if the user tries to upload the large size file or the user uploads the file using the low bandwidth facility, by default it will increase the file uploading time. Hence the time taken to upload the file and server response time are not considered in this research work.

6.1 Testing data set details

The word file, excel file, power point file, GIF image file and JPG image file types have been taken into the ACDBM for testing purpose. In each data type, five different file sizes i.e. five different cases have been taken into testing purpose to verify and evaluate the time taken and resource utilization. This is to check the time taken and resource utilization to back up the different file types with different file sizes in ACDBM's IDOCA and ODOCA modes.

6.2 Test case file sizes details

Case 1: Table 1 shows the different word document files and their file size, which are used for backup testing in ACDBM's IDOCA mode and ODOCA mode.

Case 2: Table 2 shows the different excel files and their file size, which are used for backup testing in ACDBM's IDOCA mode and ODOCA mode.

Case 3: Table 3 shows the different PDF files and their file size, which are used for backup testing in ACDBM's IDOCA mode and ODOCA mode.

Case 4: Table 4 shows the different GIF format image files and their file size, which are used for backup testing in ACDBM's IDOCA mode and ODOCA mode.

Table 1. Test Files Used for Backup Testing Purpose in IDOCA Mode and ODOCA Mode.

Sl. No.	File Name	File Size
1W	Springertemplate.docx	102 Kb
2W	CONSEG - 2015.docx	121 Kb
3W	File system watcher NEW.docx	736 Kb
4W	DTI Springer Format.docx	1196 Kb
5W	Full Contents.docx	1321 Kb

Table 2. Test Files Used for Backup Testing Purpose in IDOCA Mode and ODOCA Mode

Sl. No.	File Name	File Size
1E	WORKERS LIST.xlsx	194 Kb
2E	3D Master Indicator File.xlsx	206 Kb
3E	3D MASTER Indicators - Prototype.xlsx	623 Kb
4E	3D Factory Data.xlsx	2293 kb
5E	list_indexed_journals.xlsx	14014 kb

Table 3. Test Files Used for Backup Testing Purpose in IDOCA Mode and ODOCA Mode

Sl. No.	File Name	File Size
1P	utsa09.pdf	440 Kb
2P	ALTER-Net slide template.pdf	1308 Kb
3P	Cybersafety_basics.pdf	2715 Kb
4P	Living wage economies.pdf	3916 Kb
5P	good+DES.pdf	4702 Kb

Table 4. Test Files Used for Backup Testing Purpose in IDOCA Mode and ODOCA Mode

Sl. No.	File Name	File Size
1IG	Cat-party.gif	237 Kb
2IG	Pronounce-gif.gif	483 Kb
3IG	giphy.gif	1248 Kb
4IG	P1B20032611……map_mgdr.gif	3896 Kb
5IG	Time_02_2180x720…..TP-3.gif	9092 Kb

Table 5. Test Files Used for Backup Testing Purpose in IDOCA Mode and ODOCA Mode

Sl. No.	File Name	File Size
1IJ	ey-cloud-trust-....-framework.jpg	197 Kb
2IJ	4 X 4.jpg	521 Kb
3IJ	Cloud-need-data.jpg	1079 Kb
4IJ	Cloud-comput.…6000x4455.jpg	2245 Kb
5IJ	IMG_0404.jpg	6203 Kb

* Kb = Kilo Bytes

Case 5: Table 5 shows the different JPG format image files and their file size, which are used for backup testing in ACDBM's IDOCA mode and ODOCA mode.

6.3 Testing scenario

The above-mentioned different file types with different file sizes were tested in the lab environment level. The coding has been done in Java version 1.8 and testing is done in Core i3 3.3 GHZ processor with 4 GB RAM system. The time

consumption and resource utilization to back up the file in ACDBM server and CSP's server have been taken as a testing and evaluation parameter. The existing data backup methods are used for different purposes in different places. If the user's need is different then the user's requirement will also be different. The ACDBM has been compared only between its IDOCA mode and ODOCA mode, because the purpose of this ACDBM is different when compared to other existing models. The total numbers of testing done on the proposed ACDBM is shown below.

5 Diff. File Types	**X**	**5** Diff. File Sizes	**X**	**2** Diff. Data File Handling Modes	=	**50 Times The ACDBM Was Processed**

6.4 Time consumption details

Time consumption is used to measure and verify the efficiency between the IDOCA and ODOCA. The time consumption for the different cases, i.e. Case 1, Case 2, Case 3, Case 4, and Case 5 is shown below. The test case files sizes are different from each and every file in its own test case and files in other test cases too. The Test Cases time consumption comparisons are as follows.

Case 1: The Table 6 and Fig. 5 show the time taken in nanoseconds for five different word document files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 2: The Table 7 and Fig. 6 show the time taken in nanoseconds for five different excel files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 3: The Table 8 and Fig. 7 shows the time taken in nanoseconds for five different PDF files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 4: The Table 9 and Fig. 8 show the time taken in nanoseconds for five different GIF format image files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 5: The Table 10 and Fig. 9 show the time taken in nanoseconds for five different JPG format image files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Table 6. Time Analysis for Backup in ACDBM and CSP Server between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (ns)	ODOCA (ns)
1W	14000103	29603204
2W	11500065	30135953
3W	12711951	46821314
4W	13746720	62659640
5W	14290922	63259995

* ns = nanoseconds

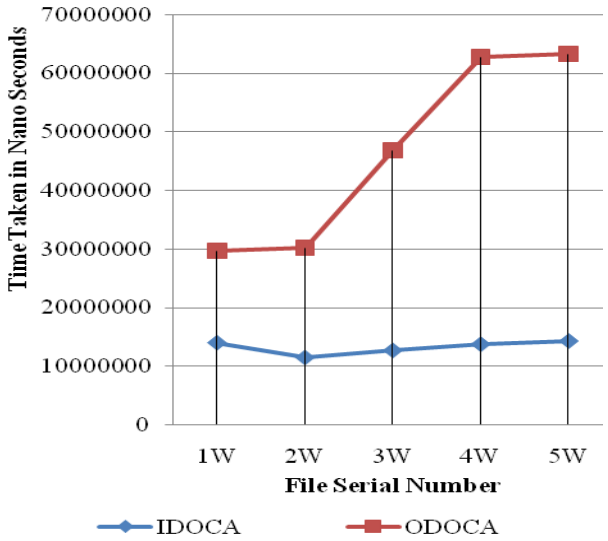

Figure.5 Time Analysis for Backup in ACDBM and CSP server between IDOCA Mode and ODOCA Mode

Table 7. Time Analysis for Backup in ACDBM and CSP Server between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (ns)	ODOCA (ns)
1E	14357690	34787382
2E	11677462	35084626
3E	12755811	46557034
4E	16307380	72170645
5E	429155661	657634699

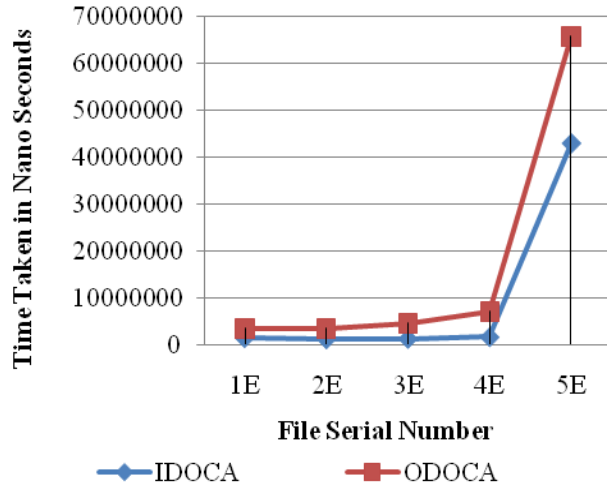

Figure.6 Time Analysis for Backup in ACDBM and CSP server between IDOCA Mode and ODOCA Mode

Table 8. Time Analysis for Backup in ACDBM and CSP Server between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (ns)	ODOCA (ns)
1P	12455214	38068246
2P	16988472	76929051
3P	23284245	116080675
4P	15303341	46515688
5P	19769630	89414157

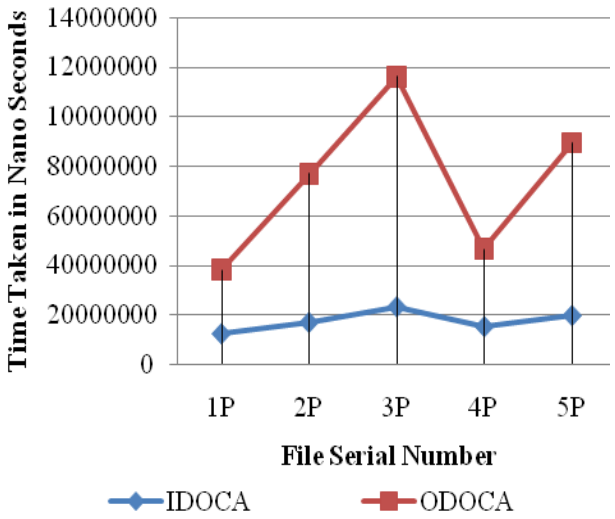

Figure.7 Time Analysis for Backup in ACDBM and CSP server between IDOCA Mode and ODOCA Mode

Table 9. Time Analysis for Backup in ACDBM and CSP Server between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (ns)	ODOCA (ns)
1IG	12618084	28134302
2IG	12774249	32181185
3IG	15186867	45817835
4IG	20062885	89595745
5IG	28682976	297084964

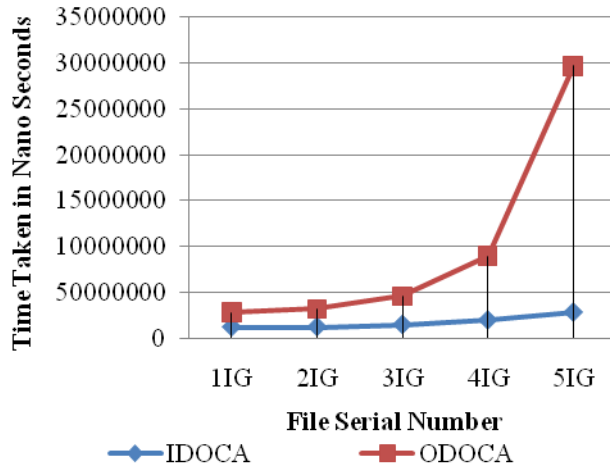

Figure.8 Time Analysis for Backup in ACDBM and CSP server between IDOCA Mode and ODOCA Mode

Table 10. Time Analysis for Backup in ACDBM and CSP Server between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (ns)	ODOCA (ns)
1IJ	13443888	28070328
2IJ	15087951	33534709
3IJ	15191596	42195865
4IJ	18002008	62035259
5IJ	25421108	126835114

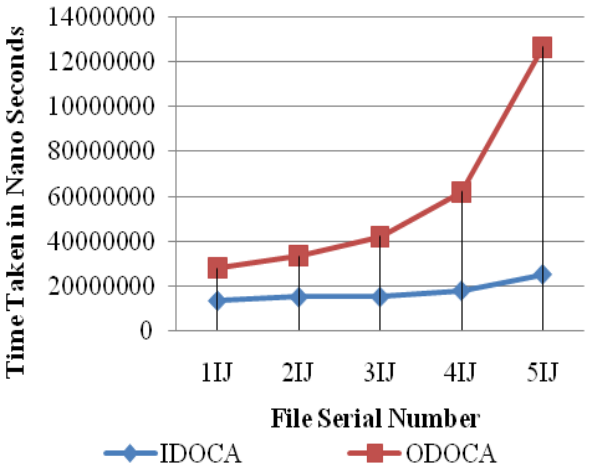

Figure.9 Time Analysis for Backup in ACDBM and CSP server between IDOCA Mode and ODOCA Mode

6.5 Resource utilization details

Resource utilization is used to measure and verify the efficiency between the IDOCA and ODOCA. The resource utilization for the different cases, i.e. Case 1, Case 2, Case 3, Case 4, and Case 5 is shown below. Both the IDOCA and ODOCA are ACDBM data transferring methods.

The test case files sizes are different from each and every file in its own test case and files in other test cases too. The Test Cases resource utilization comparisons are as follows.

Case 1: The Table 11 and Fig. 10 show the resource utilization in kilo bytes for five different word document files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 2: The Table 12 and Fig. 11 show the resource utilization in kilo bytes for five different excel files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 3: The Table 13 and Fig. 12 show the resource utilization in kilo bytes for five different PDF files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 4: The Table 14 and Fig. 13 show the resource utilization in kilo bytes for five different

GIF format image files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Case 5: The Table 15 and Fig. 14 show the resource utilization in kilo bytes for five different JPG format image files backup in ACDBM server and CSP server in IDOCA and ODOCA mode.

Table 11. Resource Utilization between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (kB)	ODOCA (kB)
1W	296080	477008
2W	296080	477152
3W	296080	477024
4W	296080	477008
5W	296080	477152

* kB = kilobytes

Figure.10 Graph for Resource Utilization between IDOCA Mode and ODOCA Mode

Table 12. Resource Utilization between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (kB)	ODOCA (kB)
1E	296080	477152
2E	296080	477048
3E	296080	477104
4E	296080	477008
5E	296080	477000

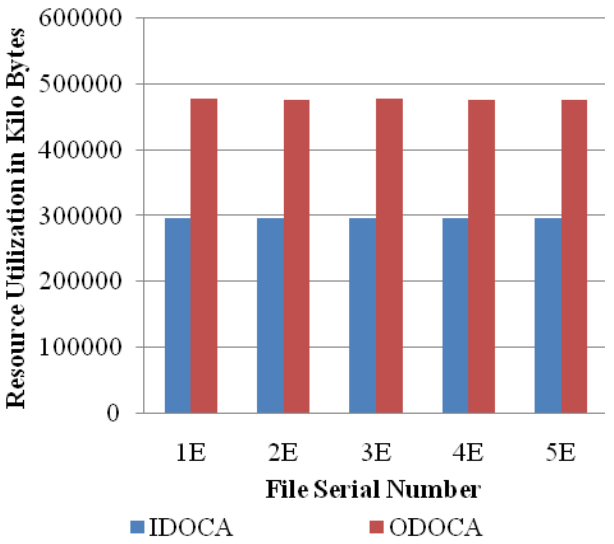

Figure.11 Graph for Resource Utilization between IDOCA Mode and ODOCA Mode

Table 13. Resource Utilization between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (kB)	ODOCA (kB)
1P	296080	477128
2P	296080	477032
3P	296080	477104
4P	296080	477048
5P	296080	477000

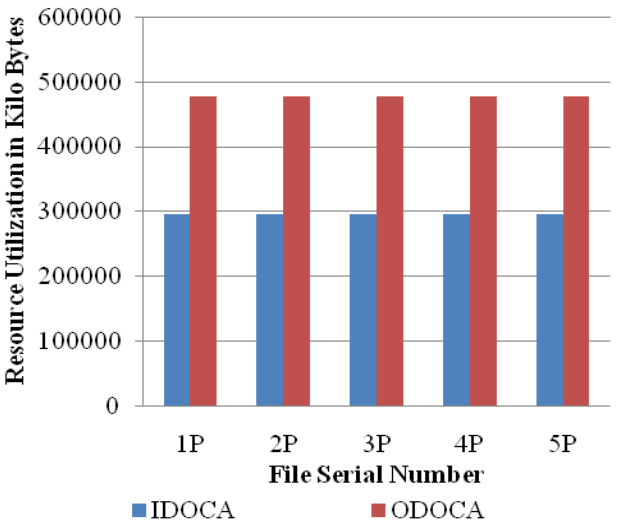

Figure.12 Graph for Resource Utilization between IDOCA Mode and ODOCA Mode

Table 14. Resource Utilization between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (kB)	ODOCA (kB)
1IG	296080	477104
2IG	296080	477104
3IG	296080	477128
4IG	296080	477128
5IG	296080	477104

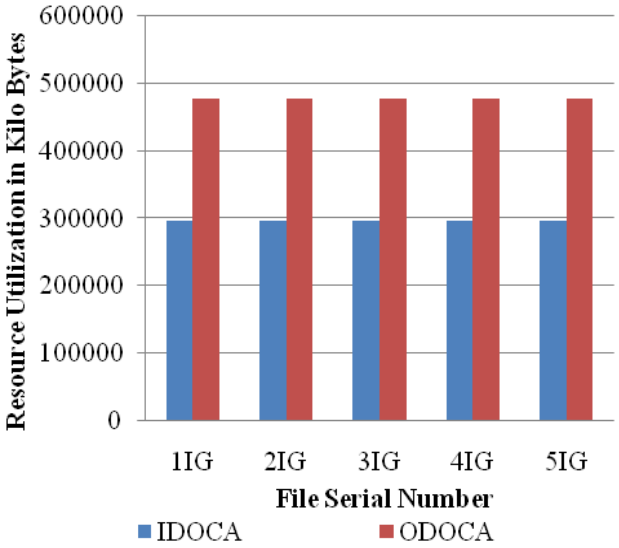

Figure.13 Graph for Resource Utilization between IDOCA Mode and ODOCA Mode

Table 15. Resource Utilization between IDOCA Mode and ODOCA Mode

File Sl. No.	IDOCA (kB)	ODOCA (kB)
1IJ	296080	477152
2IJ	296080	477128
3IJ	296080	477008
4IJ	296080	477008
5IJ	296080	477104

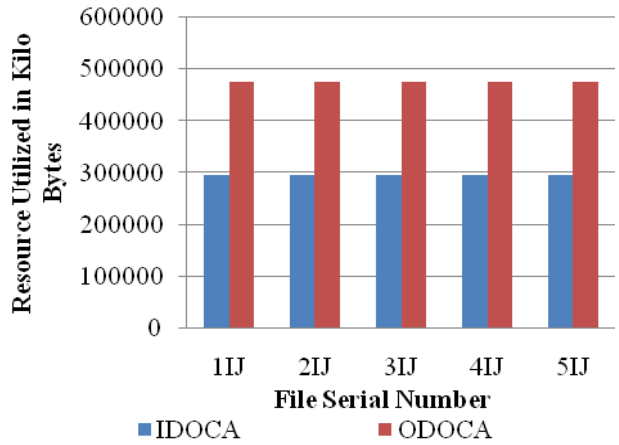

Figure.14 Graph for Resource Utilization between IDOCA Mode and ODOCA Mode

6.6 Comparison with other backup methods

The cloud backup, online backup and off-site backup are some of the existing internet-based online backup methods. When comparing the proposed Automatic Cloud Data Backup Method with existing methods, the proposed method has some more advantages than the existing methods. The advantages of proposed ACDBM are:

- The Data Handling Permission Mode as per the Data Accessing Region: ACDBM provides two different types of data accessing and handling permission to its users. But in the existing methods there is no such Data Handling Permission Mode as per the data accessing region. Moreover, unauthorized person who knows the user's security credentials can access and handle the data easily in the existing methods. But in ACDBM the authentication and other security credentials are taken care of by SCDSPM's AARM module.
- IDOCA mode allows the users to handle the data in hassle free manner. But in the existing methods all the users who have satisfied the security credentials will have all the rights on the data which are stored in online. This shows that users always will have some doubt on TRUST on their cloud service providers. This issue will not arise in ACDBM with SCDSPM's AARM and DTI&EVM modules.
- ODOCA mode allows the users to handle the data with some limitations i.e., deleting the data and storing the modification of the original data are prohibited things. It is also missing in the existing methods. When the user satisfies the security credentials in existing methods then they can create, modify and delete the data stored in online. The user identification systems in the data storage levels are not able to identify the person who satisfies the security credentials is the right one or not. So in some cases, the stolen security credentials will lead to some critical issues on online-stored data.

Data Handling Permission Mode with IDOCA and ODOCA will lead to build and maintain the TRUST between the users and its cloud service providers at the time of the users accessing their data within and outside the data ownership country. The proposed algorithms generate the backup files in algorithm designed format.

When one of the data backups is store within the user's country, then the jurisdiction issues based on data modification will come to an end. The original data don't get affected by means of any unauthorized changes from outside the data ownership country access. Also, if any unauthorized changes on original data within data ownership country access, then that unauthorized user will be bound within this country jurisdiction easily. When comparing the proposed ACDBM with the existing backup methods, the existing methods do not have country-based permission allocation and also not

permitting its users to handle the cloud data in country-based data handling modes.

7. Conclusion and future enhancement

The existing data backup methods are designed and developed for specific purposes and also each working method differs from other methods. The ACDBM is designed for the SCDSPM, and the purpose of ACDBM is to create and maintain the trust. The country level proposed ACDBM will use the local government regulations and authority standards. It will avoid the data-related threats and their related issues in cloud storage. The proposed ACDBM uses the Inside Data Ownership Country Access and Outside Data Ownership Country Access too in order to store, access and retrieve the data from cloud storage. It is a new paradigm to maintain the security and to create the TRUST between the cloud users and their cloud service providers. In future the region-based data access rights will also be considered in SCDSPM to avoid and control the unauthorized and unwanted data accesses. The ACDBM is working properly in the individual experiments and this method will need to couple with the SCDSPM's other sub-modules for finite process. And only then the SCDSPM will come into the real time usage.

References

[1] http://www.oxforddictionaries.com/definition/english/cloud-computing, Accessed: 05-05-2017.

[2] B. Duraisamy and M. Sundaresan, "Policy Based Data Encryption Mechanism Framework Model for Data Storage in Public Cloud Service Deployment Model", In: *Proceedings of 2013 Elsevier Fourth International Joint Conference on Advances in Computer Science* , Haryana, India, pp.423–429, 2013.

[3] B. Duraisamy and M. Sundaresan, "Securing Public Data Storage in Cloud Environment", In: *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India*, Visakhapatnam, India, pp.555-562, 2013.

[4] http://www.emc.com/collateral/software/white-papers/ar-backup-and-recovery-changes-drive-it.pdf, Accessed: 15-05-2017.

[5] K. Burda, "Mathematical Model of Data Backup and Recovery", *International Journal of Computer Science and Network Security*, Vol.14, No.7, pp.16–25, 2014.

[6] B. Duraisamy and M. Sundaresan, "Data Encryption Framework Model with Watermark Security for Data Storage in Public Cloud Model", In: *Proceedings of 2014 IEEE Eighth International Conference on Computing for Sustainable Global Development*, New Delhi, India, pp.1040–1044, 2014.

[7] K. Sharma and K.R. Singh, "Online Data Back-up and Disaster Recovery Techniques in Cloud Computing: A Review", *International Journal of Engineering and Innovative Technology*, Vol. 2, Issue. 5, pp.249–254, 2012.

[8] L. Xiao-lei, Z. Yong, and X. Ru-zhi. "Research On Data Backup And Recovery Technology In SCADA System", In. *Proceedings of the 2009 International Symposium on Web Information Systems and Applications,* Nanchang, P. R. China, May 22-24, pp.500-503, 2009.

[9] B. Duraisamy and M. Sundaresan, "Enhanced Encryption and Decryption Gateway Model for Cloud Data Security in Cloud Storage", In: *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of Computer Society of India*, Hyderabad, India, pp.415–421, 2014.

[10] B. Duraisamy and M. Sundaresan, "Secured Cloud Data Storage – Prototype Trust Model for Public Cloud Storage", In: *Proceedings of International Conference on Information and Communication Technology for Sustainable Development,* Ahmadabad, India, pp.329–337, 2015.

[11] B. Duraisamy and M. Sundaresan, "Framework Model and Algorithm of Request based One Time Passkey (ROTP) Mechanism to Authenticate Cloud Users in Secured Way", In: *3rd International Conference on Computing for Sustainable Global Development,* New Delhi, India, pp.5317–5322, 2016.

[12] B. Duraisamy and M. Sundaresan, "A Framework for User Authentication and Authorization using Request based One Time Passkey and User Active Session Identification", *International Journal of Computer applications,* Vol.172, No.10, pp.18–23, 2017.

[13] http://typesofbackup.com/, Accessed: 18-05-2017.

[14] S. Kadry, M. Smaili, H. Kassem, and H. Hayek, "A New Technique to Backup and Restore DBMS using XML and .NET Technologies", *International Journal on Computer Science and Engineering,* Vol.02, No.04, pp.1092-1102, 2010.

[15] R.V. Gandhi, M Seshaiah, A. Srinivas and C. ReddiNeelima, "Data Back-Up and Recovery Techniques for Cloud Server Using Seed Block Algorithm", *International Journal of*

Engineering Research and Applications, Vol. 5, Issue 2 (P-3), pp.89-93, 2015.
[16] http://www.backup4all.com/kb/backup-types-115.html, Accessed: 25-05-2017.
[17] https://en.wikipedia.org/wiki/Backup, Accessed: 12-05-2017.
[18] T. Singh, P.S. Sandhu, and H.S. Bhatti, "Replication of Data in Database Systems for Backup and Failover – An Overview", *International Journal of Computer and Communication Engineering,* Vol.2, No.4, pp. 535–538, 2013.
[19] Y. Gu, D. Wang, and C. Liu, "DR-Cloud: Multi-Cloud Based Disaster Recovery Service", *Tsinghua Science and Technology,* Vol.19, No.1, pp.13-23, 2014.