Drops (division and replication of data In cloud for optimal performance and security)

Ganesh G[1], Gurukiran S[2], Ashutosh Kumar Singh[3], Basavaraj [4] , Mr.Raghvendra K[5]

[1,2,3,4]Student, Dept. of Computer Science and Engineering National Institute of Engineering, Mysuru, India.
[5]Assisstant Professor, M.Tech from VTU belgavi, karnataka.

Abstract

Outsourcing data to third party administrative control ,as is done in cloud computing ,gives rise to security concern.The data insecurity may occur due to attacks by the other users and nodes in the cloud..Therefore, high security measures are required to protect data that collectively approaches security and performance issues.We divide the file into fragments and replicate the fragmented data over the cloud nodes.Each of the nodes store only a single fragment of a particular file that ensures even in case of a successful attack, no meaningful information is revealed to attacker.We show that the probability to locate and compromise all of the nodes storing the fragments of a single file is extremely low.

Keywords*—cloud security, fragmentation, replication, performance (key words)*

I. INTRODUCTION

Cloud computing is characterised by on-demand self-services, ubiquitous network accesses, resource pooling, elasticity, and measured services. The aforesaid characteristics of cloud computing make it a striking candidate for businesses, organizations, and individual users for adoption. The Security is one of the most crucial aspects among those prohibiting the wide-spread adoption of cloud computing. For a cloud to be secure, all of the participating entities must be secure.The data outsourced to a public cloud must be secured. unrecognised data access by other users and processes (whether accidental or deliberate) must be prevented.In this project, we propose division and Replication of Data in the cloud for Optimal Performance and Security that collectively approaches the security and performance issues In the DROPS methodology, we divide a file in to fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores solely one fragment of an information file that ensures that even just in case of a thriving attacks there is no meaty info is unconcealed to the attackers.The objective of this project is to develop the application which implements DROPS to provide security to the file stored in public cloud from the attackers. The aim of this project is to provide the security to the file stored in public cloud from the attackers The off-site data storage cloud utility requires users to move data in cloud's virtualised and shared environment that may result in various security concerns. Pooling and elasticity of a cloud resources, allows the physical resources to be shared among many users Moreover, the shared resources may be reassigned to other users at some instance of time that may result in data compromise through data recovery method Furthermore, a multi-tenant virtualised environment may result in a VM to escape the bounds of virtual machine monitor (VMM). The escaped VM can interfere with other VMs to have access to unofficial data [9]. Similarly, cross-tenant virtualised network access may also compromise data privacy and integrity. Improper media sanitisation can also leak.

II. Related Work

The Cloud Data Outsourcing in cloud computing, require high security measures as the data may be tampered by illegal users or attackers. This may have an effect on the performance of cloud, as an increase in retrieval time of data. While applying the protection measures it's needed to require into consideration the retrieval time of information. In this paper, both the issues are tried to overcome by scattering the data file over the cloud nodes. The cloud nodes store solely a fraction of the file that is split into multiple fragments.The cloud nodes are aligned with certain distance using the concept T-coloring where anattacker is unable to track the next node. To improvethe retrieval time the fragments are replicated overthe nodes which are remained by placing

thefragments. To enhance the safety normal thefragmented file is encrypted before placement oncloud node. An auditing theme is used whichcontinually monitor the cloud nodes.

If any damageoccurs the auditing system regenerate the info. Thissystem provides security and auditing of cloud data The data compromise may occur due to attacks by other users and nodes within the cloud. Therefore, high security measures arerequired to safeguard knowledge at intervals the cloud. However, the used security strategy should additionally take under consideration the optimizationof the info retrieval time.

In this paper, we propose Division and Replication of Data in the Cloud for Optimal Performance andSecurity (DROPS) that collectively approaches the security and performance issues. In the DROPS methodology, we divide afile into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragmentof a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to theattacker. Moreover, the nodes storing the fragments ar separated with sure distance by suggests that of graph T-coloring to prohibitan offender of dead reckoning the locations of the fragments. Furthermore, the DROPS methodology doesn't consider the traditionalcryptographic techniques for the information security; thereby relieving the system of computationally pricey methodologies. Weshow that the likelihood to find and compromise all of the nodes storing the fragments of one file is extraordinarily low. Wealso compare the performance of the DROPS methodology with ten other schemes.

The higher level of security with slightperformance overhead was observed Cyber infrastructures are highly vulnerable to intrusions and other threats. The main challenges in cloud computing are failure of data centres and recovery of lost data and providing a data security system.

This paper has proposed a Virtualization and Data Recovery to create a virtual environment and recover the lost data from data servers and agents for providing data security in a cloud environment. A Cloud Manager is used to manage the virtualization and to handle the fault. Erasure code algorithm is used to recover the data which initially separates the data into n parts and then encrypts and stores in data servers.

The semi trusted third party and the malware changes made in data stored in data centres can be identified by Artificial Intelligent methods using agents. Java Agent Development Framework (JADE) is a tool to develop agents and facilitates the communication between agents and allows the computing services in the system. The framework designed and implemented in the programming language JAVA as gateway orfirewall to recover the data loss.

III. EXISTING SYSTEM

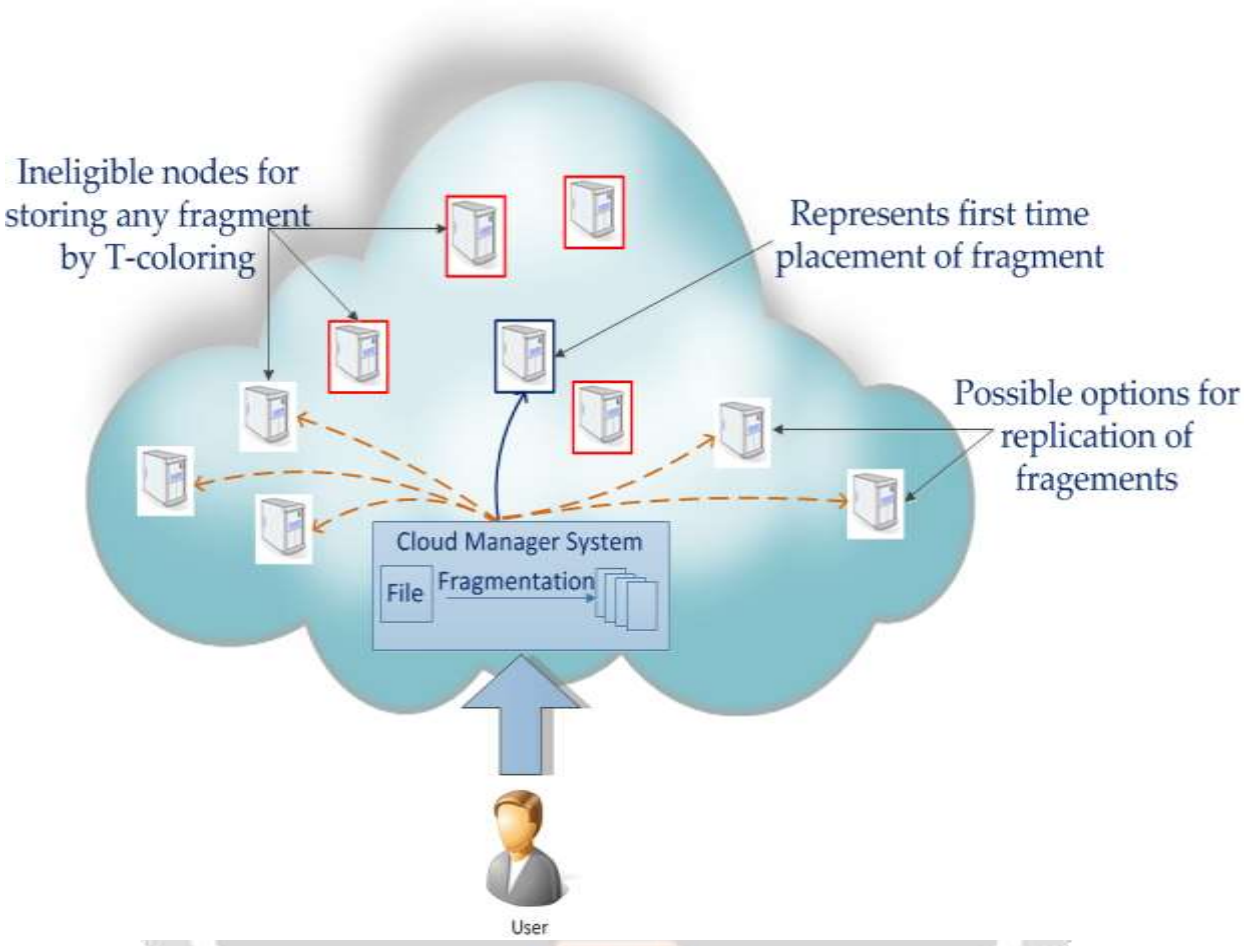
The Cloud storage is a cloud computing model in which data is stored on remote servers accessed from the Internet, or “cloud. It is maintained, operated and managed by a cloud storage service provider on a storage servers that are built on virtualisation techniques. This cloud is public , the user can store the file in the cloud storage and also provide the security to the file by encrypting the file.

Disadvantages of Previous Approach

If the attacker get the decryption key, he can able to get whole file content , which might be the confidential. If the cloud server fails , user will lose the files stored in the cloud storage , because of there is no replication of the file.

IV. PROPOSED SYSTEM

Methodology



We present DROPS that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.he division of a file into fragments is performed supported a given user criteria specified the individual fragments don't contain any significant data.A flourishing attack on a single node should not reveal the locations of different fragments at intervals the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and area unit at sure distance from one another.

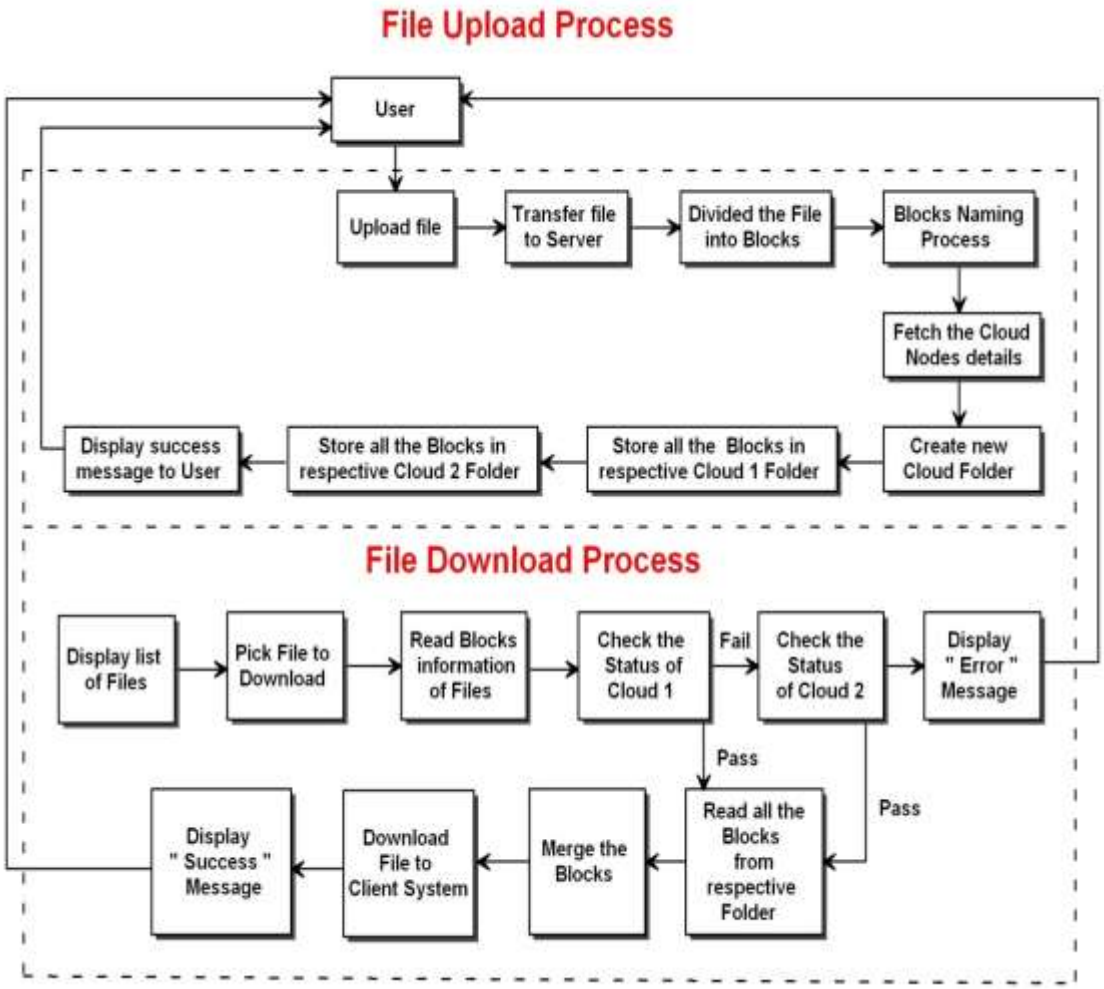
The planned theme fragments and replicates the info file over cloud nodes.The proposed DROPS scheme ensures that even in the case of a successful attack, no meaningful information is revealed to the attacker.We do not rely on traditional cryptographic techniques for data security.The non-cryptographic nature of the proposed scheme makes it faster to perform the required operations (placement and retrieval) on the info.We guarantee a controlled replication of the file fragments, wherever every of the fragments is replicated just the once for the aim of improved security.

V. SYSTEM ANALYSIS AND DESIGN

The purpose of arrangening|the look} section is to plan an answer of the matter mere by the necessities document. This section is that the opening in moving from the matter domain to the answer domain. In alternative words, starting with what is needed; design takes us toward how to satisfy the needs.

The design of a system is perhaps the most critical factor affecting the quality of the software; it has a major impact on the later phases particularly testing and maintenanceBlowfish is an encryption algorithm that can be used as a replacement for the DES or IDEAalgorithms. It is a symmetric (that is, a secret or private key) block cipher that uses a variable-length key, from 32 bits to 448 bits, making it useful for both domestic and exportable use. (The U. S. government forbids the exportation of cryptography code mistreatment keys larger than forty bits except in special cases.)

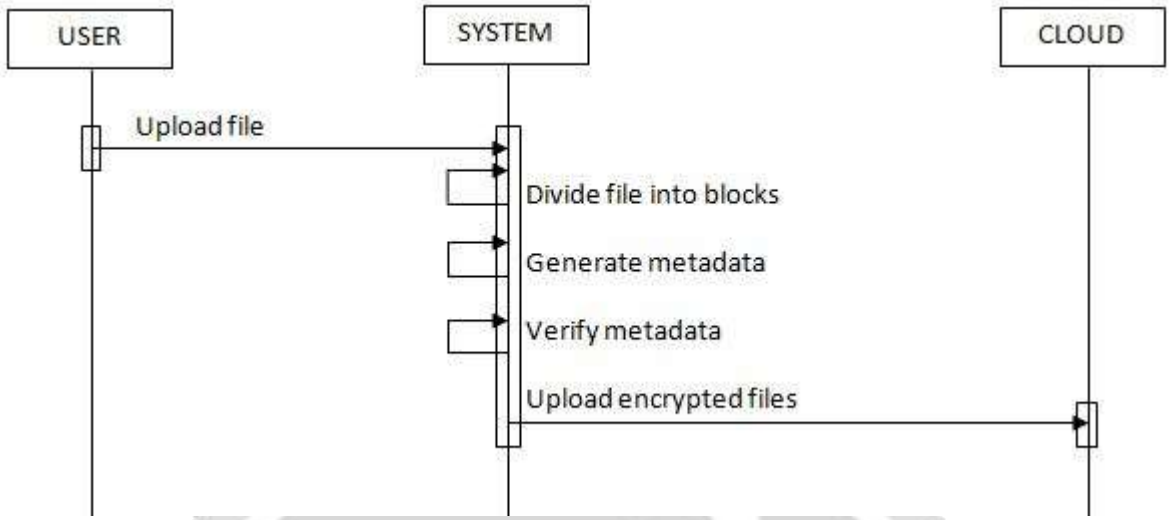
Blowfish was designed in 1993 by Bruce Schneier as another to existing cryptography algorithms. Designed with 32-bit instruction processors in mind, it is significantly faster than DES. Since its origin, it has been analyzed considerably. Blowfish is unpatented, license-free, and available free for all uses.Many cryptographers have examined Blowfish, although there are few published results. Everyone is welcome to transfer Blowfish and use it in their application. There aren't any rules concerning use, though i'd appreciate being notified of any business applications mistreatment the merchandise in order that I will list them on this web site.System architecture



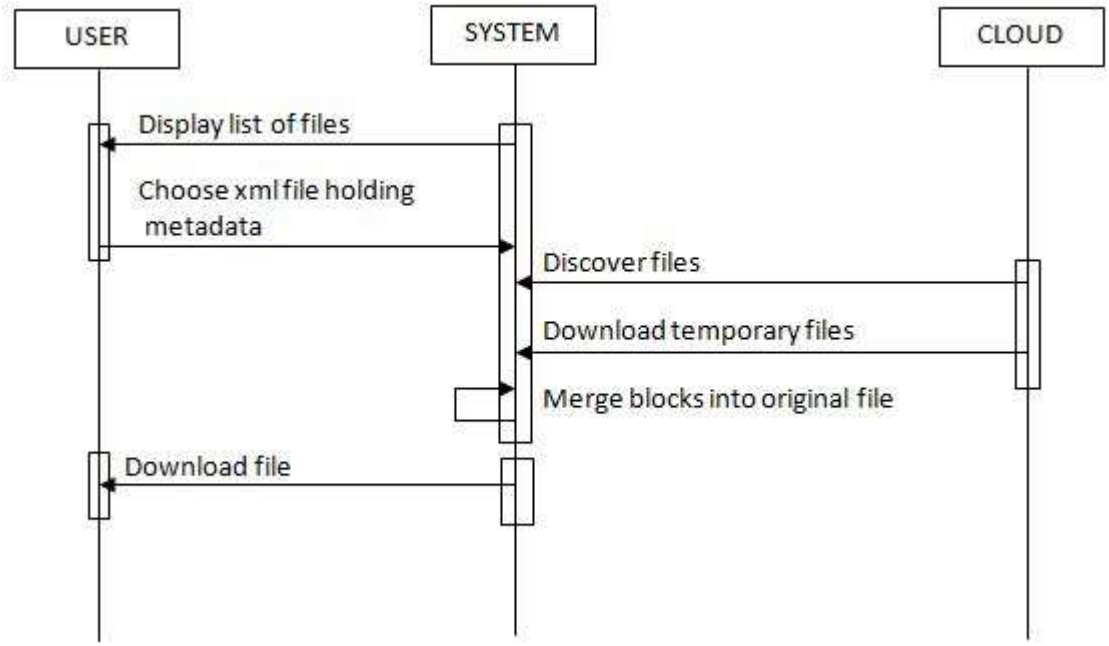
Asymmetric key algorithm

It is relatively a new concept unlike symmetric cryptosystem. Different keys are used for encryption and decryption. This is a property that set this theme totally different than bilaterally symmetrical cryptography theme. Each receiver possesses a coding key of its own, typically remarked as his non-public key. Receiver must generate associate degree cryptography key, remarked as his public key. Generally, this type of cryptosystem involves trusted third party which officially declares that a particular public key belongs to a specific person or entity only.

Sequence Diagram for uploading process



Sequence Diagram for downloading process



System model

Consider a cloud environment, a file in its totality, stored at a node leads to a single point of failure successful attack on a node might put the data con- fidentiality or integrity, or both at risk. The same situation will occur each within the case of intrusion or accidental errors. In such systems, performance in terms of

retrieval time can be enhanced by employing replication strategies. However, replication increases the number of file copies within the cloud. Thereby, increasing the probability of the node holding the file to be a victim of attack as discussed in Section 1.

Security and replication are essential for a large-scale system, such as cloud, as both are utilized to provide services to the end user. Security and replication should be balanced such one service should not lower the service level of the opposite. In the DROPS methodology, we propose not to store the entire file at a single node. The DROPS methodology fragments the file and makes use of the cloud for replication.

The fragments square measure distributed such no node in a very cloud holds over one fragment, so that even a successful attack on the node leaks no significant information. The DROPS methodology uses controlled replication wherever every of the fragments is replicated one time within the cloud to enhance the safety. Although, the controlled repli- cation does not improve the retrieval time to the level of full-scale replication, it significantly improves the security.

In the DROPS methodology, user sends the data file to cloud. The cloud manager system (a user facing server in the cloud that entertains user's requests) upon receiving the file performs: (a) fragmentation, (b) first cycle of nodes selection and stores one frag- ment over every of the chosen node, and (c) second cycle of nodes selection for fragments replication.

The cloud manager keeps record of the fragment placement and is assumed to be a secure entity. The fragmentation threshold of the data file is spec- ified to be generated by the file owner. The file owner will specify the fragmentation threshold in terms of either proportion or the amount and size of various fragments.

The percentage fragmentation threshold, for instance, can dictate that each fragment will be of 5% size of the total size of the file. Alternatively, the owner may generate a separate file containing information about the fragment number and size, for instance, fragment 1 of size 5,000 Bytes, fragment 2 of size 8,749 Bytes. We argue that the owner of the file is the best candidate to generate fragmentation threshold. The owner will best split the file such every fragment doesn't contain vital quantity of data because the owner is cognizant of all the facts relating the data.The default percentage fragmentation threshold can be made a part of the Service Level Agreement (SLA), if the user does not specify the fragmentation threshold while uploading the data file. We primarily focus the storage system security during this work with AN assumption that the channel between user and therefore the cloud .

Algorithm

Inputs and initializations:

$O = \{O_1, O_2, ..., O_N\}$
$o = \{sizeof(O_1), sizeof(O_2), ..., sizeof(O_N)\}$ *col* = {open color, close color}
$cen = \{cen_1, cen_2, ..., cen_M\}$
col ← open color∀ i
cen ← cen_i∀ i
Compute:
foreach $O_k \in O$**do**

select $S^i \mid S^i \leftarrow$ indexof(max(cen_i))
if col_{S^i} = *open color* and $s_i >= o_k$ then

$S^i \leftarrow O_k$
$s_i \leftarrow s_i - o_k$

$col_{S^i} \leftarrow$ close color

S^{i} '← distance(S^i, T)
distance T from S^i and stores in temporary set S^{i}'*/

col_{S^i} end if

end for

← close color

Work load

The size of files were generated using a uniform dis- tribution between 10Kb and 60 Kb. The primary nodes were indiscriminately elect for replication algorithms. For the DROPS methodology, the Si′s selected during the first cycle of the nodes selection by Algorithm 1 were considered as the primary nodes.

Results and Discussion

Impact of increase in number of cloud nodes

We studied the performance of the placement tech- niques and the DROPS methodology by increasing the number of nodes. The performance was studied for the three discussed cloud architectures. The numbers of nodes selected for the simulations were 100, 500, 1,024, 2,400, and 30,000. The number of nodes in the Dcell architecture increases exponentially [2]. For a Dcell architecture, with two nodes in the $Dcell_0$, the architecture consists of 2,400 nodes. However, increasing a single node in the $Dcell_0$, the total nodes increases to 30, 000 [2].

VI. FUTURE SCOPE

Several it saves the time and resources utilized in downloading, up- dating, and uploading the file again. Moreover, the implications of TCP in-cast over the DROPS methodology need to be studied that is relevant to distributed data storage and access.

VI. CONCLUSION

We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time.The data file was fragmented and the fragments are dispersed over multiple nodes. The fragmentation ANd dispersion ensured that no vital data was getable by an opposer just in case of a made attack. Fragmentation used to protect data from unity point in time disaster. No node within the cloud, stored more than a single fragment of the same file. The performance of the DROPS methodology was compared with full-scale replication techniques. The results of the simulations unconcealed that the coincidental concentrate on the protection and performance, resulted in increased security level of data accompanied by a slight performance drop.

Currently with the DROPS methodology, a user has to download the file, update the contents, and upload it again. It is strategic to develop AN automatic update mechanism which will establish and update the specified fragments solely.

REFERENCES

[1] K. Bilal, S. U. Khan, L. Zhang, H. Li, K. Hayat, S. A. Madani, N. Min-Allah, L. Wang, D. Chen, M. Iqbal, C. Z. Xu, and A. Y. Zomaya, “Quantitative comparisons of the state of the art knowledge center architectures,” Concurrency and Computation: observe and skill, Vol. 25, No. 12, 2013, pp. 1771-1783.

[2] Sujatha d, L.Blain,andJ-C.Fabre,“Intrusiontoleranceindis- tributed computing systems,” In Proceedings of IEEE Computer Society Symposium on

[3] L. M. Kaufman, “Data security in the world of cloud comput- ing,” IEEE Security and Privacy, Vol. 7, No. 4, 2009, pp. 61-64.

[4] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, “Dike:

Virtualization-aware Access Control for Multitenant Filesys- tems,” University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[5] D. Zissis and D. Lekkas, “Addressing cloud computing secu- rity issues,” Future Generation Computer Systems, Vol. 28, No. 3, 2012, pp. 583-592.

[6] A. R. Khan, M. Othman, S. A. Madani, S. U. Khan, “A survey of mobile cloud computing application models,” IEEE Communications Surveys and Tutorials, DOI: 10.1109/SURV.2013.062613.00160.

[7] G. Kappes, A. Hatzieleftheriou, and S. V. Anastasiadis, “Dike: Virtualization-aware Access Control for Multitenant Filesys- tems,” University of Ioannina, Greece, Technical Report No. DCS2013-1, 2013.

[8] Y. Tang, P. P. Lee, J. C. S. Lui, and R. Perlman, “Secure overlay cloud storage with access management and warranted deletion,” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, Nov. 2012, pp. 903-916.

[9] D.Boru, D.Kliazovich , F.Granelli, P.Bouvry,andA. Y.Zomaya, “Energy-efficient data replication in cloud computing datacen- ters,” In IEEE Globecom Workshops, 2013, pp. 446-451. .